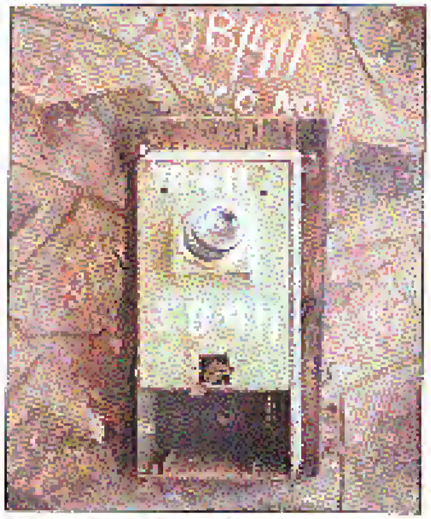
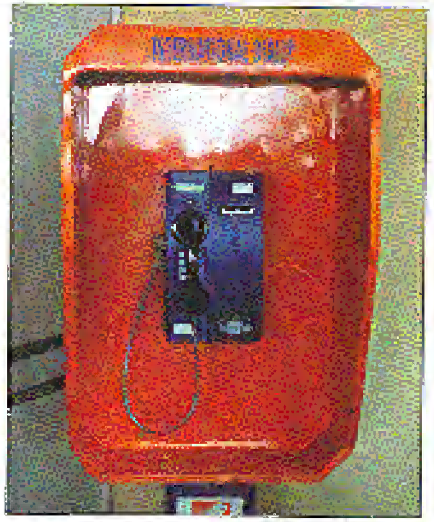
Worldly Payphones



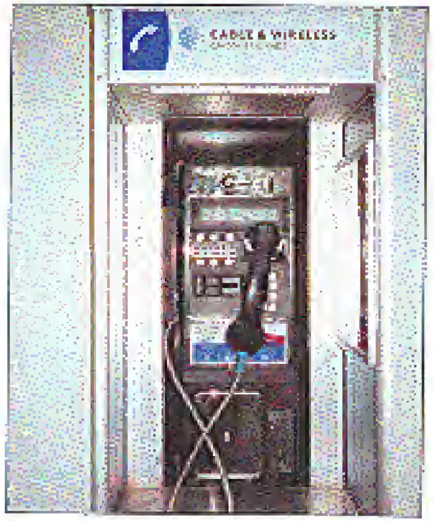
Delhi, India. That's actually a water bottle stuffed down the phone's throat. People in India take a dim view of inadequate payphones.

Photo by Tom Mele



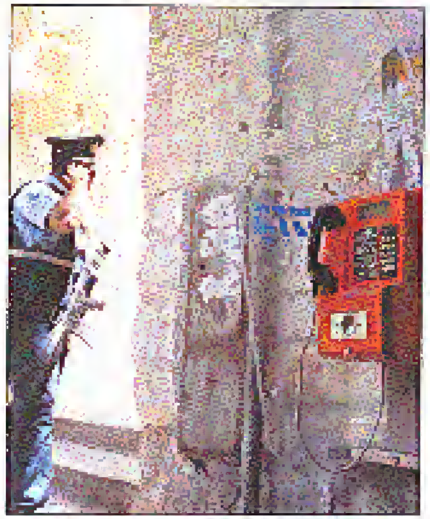
Lahore, Pakistan. This phone supposedly can go anywhere.

Photo by Tom Mele



Cayman Islands. From the Grand Cayman Island, this phone seems overly modern for such a tiny place.

Photo by Paul Benford



Jerusalem, Israel. Phones do not misbehave here. Not with that kind of enforcement.

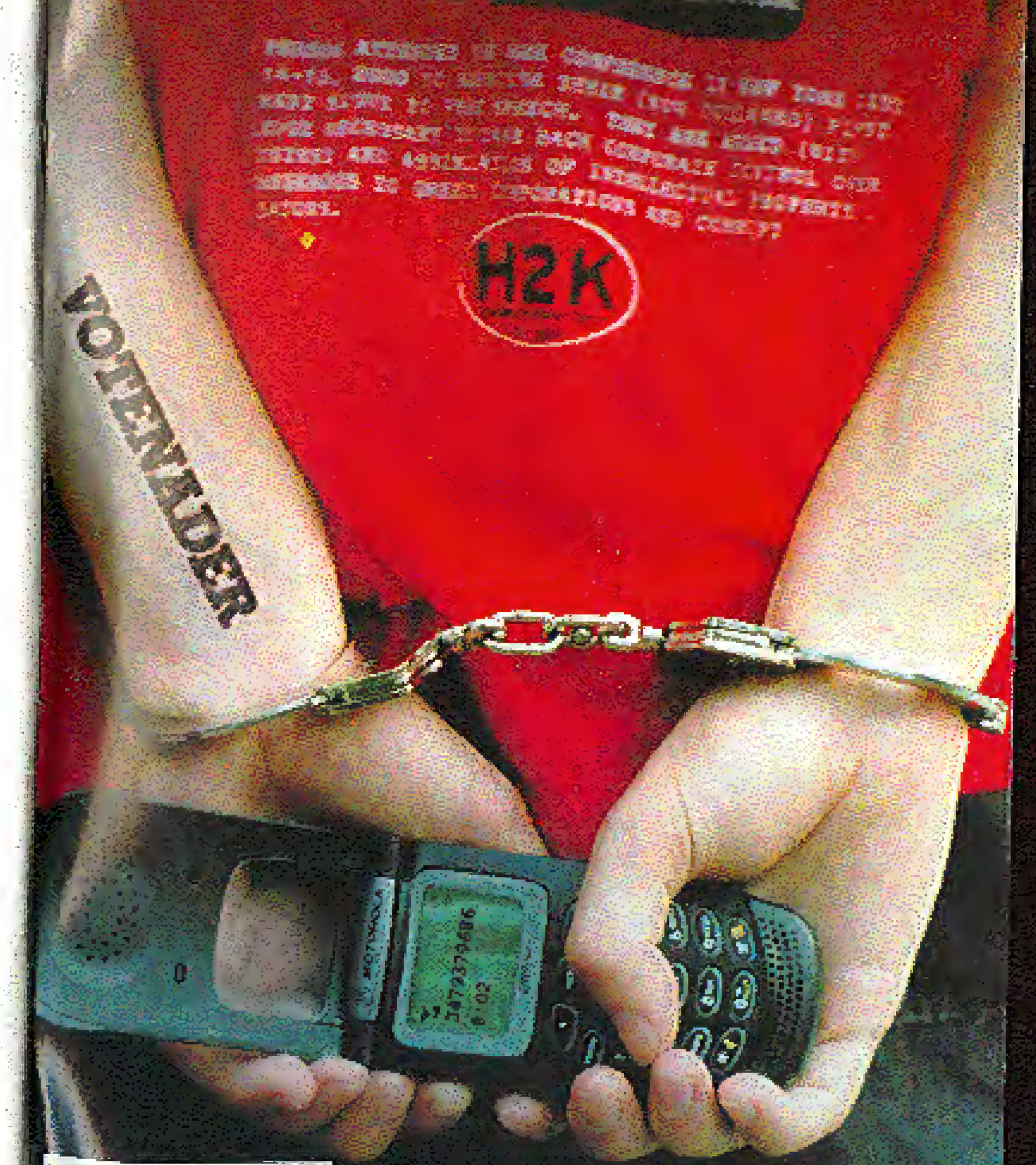
Photo by M. Cameron Newell

Come and visit our website and see our vast array of payphone photos that we've compiled! http://www.2600.com

2600

The Hacker Quarterly

Volume Seventeen, Number Three
Fall 2000
$5.00 US, $7.15 CAN



"Anyone wishing to make lawful use of a particular movie may buy or rent a videotape, play it, and even copy all or part of it with readily available equipment." - Judge Lewis A. Kaplan's way of dealing with the fact that it's virtually impossible to do this with a DVD - his apparent solution is to just go back and use old technology that isn't subject to insane laws.

S T A F F

Editor-In-Chief
Emmanuel Goldstein

Layout and Design
ShapeShifter

Cover Concept and Photo
David A. Buchwald

Cover Design
The Chopping Block Inc.

Office Manager
Tampruf

Writers: Bernie S., Billsf, Blue Whale, Noam Chomski, Eric Corley, Dr. Delam, Derneval, Nathan Dorfman, John Drake, Paul Estev, Mr. French, Thomas Icom, Javaman, Joe630, Kingpin, Miff, Kevin Mitnick, The Prophet, David Ruderman, Seraf, Silent Switchman, Scott Skinner, Mr. Upsetter

Webmaster: Macki

Network Operations: CSS

Still More Video Production: Porkchop

Broadcast Coordinators: Juintz, Cnote, Shiftlock, Silicon, Absolute0, BFmadman, BluKnight, Monarch, FearFree, Mennonite, Sardonic

IRC Admin: ross

Inspirational Music: Jean Michel Jarre, Linton Kwesi Johnson, Chappaquiddick Skyline, Giant Sand, Mercury Rev.

Shout Outs: There's no way we can give adequate credit to the scores of people who helped make H2K the memorable event it turned out to be, nor can we properly acknowledge the many who took the time to come to our trial and also those who stood outside the courthouse and demonstrated, and we can never accurately thank everyone who helped make our documentary ("Freedom Downtime") happen. And while we're at it, we have to recognize the bravery of the folks who stood up at RNC in Philadelphia and DNC in Los Angeles. All of these people have been an immense inspiration.

2600 *(ISSN 0749-3851) is published quarterly by 2600 Enterprises Inc. 7 Strong's Lane, Setauket, NY 11733. Second class postage permit paid at Setauket, New York.*

POSTMASTER: Send address changes to
2600, P.O. Box 752, Middle Island, NY 11953-0752.

Copyright (c) 2000
2600 Enterprises, Inc.

Yearly subscription: U.S. and Canada - $18 individual, $50 corporate (U.S. funds). Overseas - $26 individual, $65 corporate.

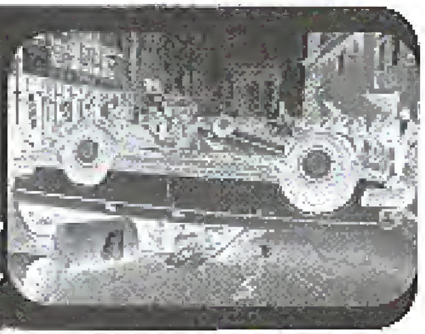
Back issues available for 1984-1999 at $20 per year, $25 per year overseas. Individual issues available from 1988 on at $5 each, $6.25 each overseas.

ADDRESS ALL SUBSCRIPTION CORRESPONDENCE TO:
2600 Subscription Dept., P.O. Box 752,
Middle Island, NY 11953-0752
(subs@2600.com).

FOR LETTERS AND ARTICLE SUBMISSIONS, WRITE TO:
2600 Editorial Dept., P.O. Box 99,
Middle Island, NY 11953-0099
(letters@2600.com,
articles@2600.com).

***2600* Office Line: 631-751-2600**
***2600* FAX Line: 631-474-2677**

HANDLE CONTENTS WITH CARE



A Summer of Trials

One thing the summer of 2000 will not be remembered for is dullness. We've never had so many different things come together at more or less the same time. Yet all of these different things were somehow related and extremely relevant to where we are headed.

Many see it as a bad thing that the DeCSS trial dominated our time as much as it did. Unfortunately, there was never a choice. Like a dangerous disease, it had to be fought with every ounce of our strength. Thanks to the support of the EFF and a terrific legal defense team, we had the best chance possible of getting our side out.

It seemed obvious from the beginning that the court was sympathetic to the case of the MPAA and this was certainly borne out in the decision. But the reaction of the many thousands who have been following this case one way or another around the globe only confirmed that we succeeded in making the points we needed to make. Anyone with a degree of knowledge in either technical issues or the value of freedom of speech seems to get it right away. Why then did our court system fail to?

We can analyze it forever. But it basically comes down to perception. The judge bought into the notion that hackers are evil and only interested in causing problems, pirating films, and bringing down corporate America. Ironically, decisions such as this do more to foster such hostility than anything else and we've seen a very definite change in tone within several communities - hackers, open source, independent artists, activists - it's rapidly turning into an us versus them scenario. And it's all but assured that someone is going to fall into the mass graves that corporate America is digging.

For those without access to the net and who may have missed it in the media, the MPAA was granted a permanent injunction against our posting the DeCSS code which allows DVDs to be played on alternative platforms such as Linux. The main thrust of the MPAA's argument was that this would also allow people to copy unencrypted DVD files and then transfer them over the net. It was demonstrated time and again that such activity would take massive time and bandwidth and that it would ultimately prove pointless since encrypted files could still be copied and read through any existing DVD player and since the cost of DVDs was low enough to make piracy a money losing venture. But this case was never about piracy. It all centered around the MPAA wanting control over how people play digital media. They want to be able to dictate how, when, and where you can access content. We're already seeing the results of this in the form of region coding (preventing the viewing of DVDs from one geographical region to another), the elimination of "fair use" which has always allowed for consumers to make personal copies of the material they've purchased, and the ability to force consumers to sit through commercials and FBI warnings without the ability to skip through them. And don't for a moment think it will stop there. You will soon see the same kind of controls introduced on audio recordings. And, with the advent of HDTV, don't be surprised when you have to pay a fee to record your favorite program and another fee for every time you want to view it. All of this is not only possible under the Digital Millennium Copyright Act (the 1998 legislation that made this lawsuit and the many that will follow possible), but increasingly likely to be only the tip of the iceberg. If the rest of the DMCA goes into effect as scheduled in late October, it will be illegal to even figure out on your own ways of circumventing these many controls and restrictions.

It's not too late to make the DMCA into a political issue. There are no voting records on its passage other than Clinton's signing it into law. Both the House and the Senate used voice votes to assure its passage. That means it's as good as unanimous. Every single elected official needs to be targeted aggressively so that they realize what a bad mistake the DMCA is. It's extremely likely many of them didn't get the full story when they were considering it. It's up to us to see that they understand it now. And if they refuse to, to replace them with someone who does.

The MPAA has gotten an immense amount of bad publicity because of this case. People who weren't even aware of who the MPAA was now think of them in a negative way. Their victory will be more costly than our loss. And ultimately they cannot hope to hold consumers hostage for very much longer. We find that once consumers become aware of what this is really about, they understand the importance of the case very quickly. That's why getting the word out to as many people as possible - leafleting, demonstrations, web pages, public forums - is so vital at this stage.

What we've seen over the last few months as a direct result of this is the tremendous growth of activism in our community. The Free Kevin movement started us in this direction and the DeCSS case gave us a real push. This in turn has gotten many more people involved and helped to solidify ties between communities that have always been fighting for the same things in different ways. Since we cannot count on the media (most of them are owned by companies who are part of the lawsuit against us) we have to do it ourselves. As Jello Biafra put it during his keynote address at H2K, we must "become the media."

All of us have that ability and the net is what makes it possible. But the net is also in danger of becoming co-opted by the same entities who are trying to shut us down. This can happen in several ways. Our best and brightest can be lured away into corporate settings where the values they once held dear are cashed in for stock options. More regulations by nervous governments can reduce the free potential of the global net to mere folklore. By portraying those in our community as criminals by focusing on absurdities like mail viruses and "potential" crimes, public opinion can be easily swayed to turn us into the enemy which makes control all the more necessary in the eyes of the masses.

One thing that seemed to come out of this summer's H2K conference was the sentiment that the time to sit back and take it is over. If we want to preserve our existing freedoms and restore those that we've already lost, the only way to accomplish this is to get involved. While it's easy to just sit back and let life happen, joining forces and working towards a goal is what makes for significant change. And it also happens to feel great.

That's precisely why this year's conference had more of an activist slant to it. While the world of hackers is ultimately about playing with technology, figuring things out, and sharing information, powerful entities have decided that these things are not to be tolerated. We find our very existence - and that of free thinkers of all sorts - threatened in ways even we find ourselves surprised by. While it's relatively simple to close one's eyes and play ball, the results would be nothing short of catastrophic. We have to take a stand and we have to be willing to pay the price.

We've seen this sentiment echoed several times this year. Three issues ago we told the story of Seattle and how for the first time independent media people used the net in a major way to report a story that the mainstream had ignored. As we suspected, it was the beginning of a trend. This summer, history repeated itself in Philadelphia and Los Angeles at the two major political conventions. Crowds were attacked in the streets by police firing rubber bullets (a practice introduced in Seattle last November), peaceful protests were made illegal, and the mainstream media dutifully went along for the ride. Suspected "leaders," including a 2600 staffperson, were hunted down and arrested, in some cases just for walking down a street with a cell phone (later defined by authorities as an implement of crime). Bail was set at up to a million dollars and people were thrown into prisons with utterly horrendous and barbaric conditions.

If you watched the news and read the papers, you probably heard the exact same words repeated over and over that would lead you to believe that these actions were somehow justified. For those who were there and for those who participated over the net, a very different story than what was being reported on the mainstream media soon revealed itself. Thanks to a new and long overdue brand of media not controlled by corporate interests and a belligerent government, firsthand accounts got out to the world in the form of video, audio, and the written word. Most of this was limited to the Internet but at least one brand new satellite channel - Free Speech TV - managed to bring this material into millions of living rooms nationwide. And, just like you would expect to see in those "uncivilized" foreign nations, the authorities came down hard on these independent media types, harassing them at every opportunity, denying them access, and even going so far as to disrupt their legitimate work. One unbelievable incident took place at the Democratic Convention in Los Angeles as the people at Free Speech TV were preparing a live broadcast. Police came in and shut down the facility because of a "bomb threat." But no

Continued on page 47

Kernel Modification Using LKMs

by dalal (dalal@insomnia.org)

This article explores the mysterious virtue of kernel modification, with particular regard toward LKMs and their use in the subject. Kernel hacking is no easy task, but well worth the trouble of learning it. If you're not yet involved in it, maybe this will catch your interest. If you are, maybe this will teach you a few things.

I'm assuming that the reader is an experienced Unix user, is fairly familiar with kernel principles and semantics, and is a C programmer. That's you, and you've used LKMs in routine administration tasks, but maybe you're not sure how they actually work? In that case, I'll begin with a crash course on the subject.

An LKM, or Loadable Kernel Module, is a system used by Linux as well as some other modern operating systems to allow the linking of object code into a running kernel without interrupting any system traffic. Most basically, an object is compiled to a relocatable object (.o) file, loaded using "insmod" under Linux, and removed using "rmmod". Linux also supports demand loading of modules, using "kerneld" (now kmod). Don't forget the man pages.

Once "insmod" is called, the module is linked into the running system kernel and the function init_module() is called. All modules must contain this function, as well as cleanup_module() which is called at unloading. The purpose of init_module() is to register the functions contained within the module to handle system events, such as to be device drivers or interrupt handlers.

The actions performed by insmod are similar to that of "ld", at least as far as linkage goes. You are free to write to your heart's content, however you may not use functions contained in libraries, such as libc. It seems like many newcomers to kernel coding don't realize this. It sounds crippling, but you can nonetheless produce some very interesting and useful modules, and without overhead of static libraries.

I've narrowed this down to two main parts: stealthing a module (to avoid detection) and utilizing basic system resources from within a module. If you're curious about anything not discussed here feel free to e-mail me at the address above.

Stealth

To effectively hide a module we should first determine where it is likely to be seen. We obviously should remove any traces of our modification from /proc/modules, and thereby lsmod. In addition, we should ensure that our functions do not appear in the kernel symbol table, /proc/ksyms. To be extra careful, we should hide the disk image after we've loaded the module into memory.

Removing a module from the system list of modules was first introduced to me in Phrack 52, in an article by Plaguez entitled "Weakening the Linux Kernel." This is an excellent article for beginners and I suggest you read it. Plaguez's technique requires little more than changing a few values in memory, which can be referenced with <linux/module.h>.

Unfortunately Plaguez's technique does not work on the newer 2.2 kernels. Earlier kernel versions contained this line in kernel/module.c which allowed his technique:

if(*q == '\0' && mp->size == 0 && mp->ref == NULL)

continue; /* don't list modules for kernel syms */

This is not present in 2.2.

To remedy this I have written what you will find below. It simply takes the specified module out of the module list, leaving the actual module in memory. The target module must have already been loaded. This will unload itself after running, so don't bother doing it.

```
--wipemod.c-----------------------------------------------
/*
 * wipemod.c
 * dalal(dalal@insomnia.org)
 *
 * usage: 'insmod wipemod name=target.o'
 *
 * Notice: The target module must already be loaded,
 * and wipemod will unload itself.  Also, because
 * it unloads itself, wipemod cannot restore a module
 * into the list after it has been taken out.
 *
 * This is built for Linux 2.2.
 *
 *             Ignore annoying secondary error messages.
 */

#include <linux/kernel.h>
#include <linux/module.h>
#include <linux/string.h>

char *name;
MODULE_PARM(name, "s");

int
init_module()
{
        struct module *lmod;

        if(name == NULL){
                        printk("<1>usage: 'insmod wipemod name=target.o'\n");
                        return 1;
        }

        while(1){
        if(!lmod->next){
                                printk("<1>Failure.  Perhaps the target module isn't
loaded?\n");
                                return 1;
                        }

                        if(!strcmp((char *) lmod->next->name, name)){
                                if(lmod->next->ndeps != 0)      /* level ndeps */
                        lmod->next->ndeps = 0;

                                lmod->next = lmod->next->next;

                                printk("<1>Success.\n");
                                return 1; /* return 1 so it will unload. */
                        }

                        lmod = lmod->next;
        }
}

void
cleanup_module()
{
     /* This will never be called. */
}
-----------------------------------------
```

This has another useful function, it can be used to remove a broken module from the listings. This is very handy when you do something wrong while creating a module and it refuses to unload, which happens more often than you may think. Running it for this purpose is not as safe as rebooting, as the module is technically still in memory, but it's much faster.

Symtabs

Keeping components of your module from being listed in ksyms used to be handled by "register_symtabs". However that has changed with newer kernel versions. There are new ways of doing this now, but why would we want to in the first place? First of all it will keep the curious system administrator from seeing something such as "hax0r_passwords()" and its address in the kernel symbol table. Second, it will keep any other module from referencing you, although that occurrence is improbable.

Selectively allowing some parts of your code to show up as ksyms can be done by simply creating the functions you wish to be hidden as "static". For instance, "static int return_vals()" would not show up, whereas "int return_vals()" would.

Alternatively, you can slip "EXPORT_NO_SYMBOLS" into your module somewhere. This is defined in <linux/module.h> as this:

#define EXPORT_NO_SYMBOLS __asm__(".section __ksymtab\n.previous")

Installing your module with "insmod -x" would also be effective, but that is boring.

Using Kernel Resources

After it has been loaded, your code of course becomes part of the kernel and can do anything. In the right hands this commodity is (root * 10). As examples of this I'll show you some interesting things that a module can do, including how to add your own system calls at runtime.

The list of exported kernel symbols (ones you can readily utilize) is located in /proc/ksyms. A more pretty version of this list can be viewed with the "ksyms" command. Note that by default "ksyms" does not display symbols from "the kernel proper." You can view all symbols with "ksyms -a".

Even though you can't directly link libraries into your module, you can do anything from kernel code that you would be able to do with any library, including libc. After all, libraries eventually rely on kernel functions to operate. As a simple example:

libc: var = getuid();

kernel: var = current->uid;

It may go understood without mention that in order to use the second example from above, <linux/sched.h> needs to be included.

You can see how some inherent system calls handle the absence of convenient library functions in the kernel source, "kernel/exit.c" for example (sys_exit).

System Calls

Much more interesting is the possibility of adding system calls to a running kernel. But why would you want to do this? Its practical use may not be as defined as its educational purpose, but it is not nonexistent. An example of possible use for this would be to provide temporary portability for compiling and running certain programs on an other than native platform. Dirty, but not without utility.

Viewing the assembly source in arch/i386/kernel/entry.S, we see that several things happen when the switch is made from user mode with the system call. Initially registers are saved. A comparison is made against the value of NR_syscalls to make sure that the requested call is within bounds, and control is passed to the system call. The actual call is indexed by numbers contained in <asm/unistd.h>, one for each system call(__NR_syscall), which reside in "void *sys_call_table[]".

Knowing the above we can implement our own system call as follows:

```
------------------------------------------
#include <linux/kernel.h>
#include <linux/module.h>
#include <linux/sys.h>
#include <stdio.h>

extern void *sys_call_table[];

asmlinkage static int sys_my_func();

void *old_val;

int
init_module()
{
                old_val = (void *) sys_call_table[250];

                sys_call_table[250] = (void *)
sys_my_func;

                return 0;
}

asmlinkage static int
sys_my_func()
{
                printk("I am a working system call.\n");
                return 0;
}

void
cleanup_module()
{
                sys_call_table[250] = old_val;
}
------------------------------------------
```

And we can call it as such:

```
__asm__("movl   $250, %eax

        int   $0x80");
```

Or with _syscall0().

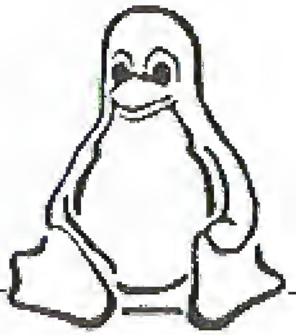
Bottom-half Handlers

Bottom-half handlers are part of the interrupt mechanism of Linux. The purpose behind them is to speed up system operation. When an interrupt occurs the main interrupt handler will typically do a small amount of work, and then return control to the OS. At a later time the interrupt's bottom-half will be executed. This is typically the bulk of the interrupt code. Doing things this way allows the system to spend a minimal amount of time within a single interrupt.

It's very possible to register our own bottom-half handlers, even without providing support for any actual interrupts. Using functions already built into the kernel, we can register a function as a bottom-half, mark it to be run, and thereby have our code executed as any real bottom-half.

But why would we want to do this? Surely by now you know to trust me when I say there's a purpose behind some weird manipulation of the kernel that I present. In this case, we do it so that a desired bit of code is executed on a relatively constant basis, so that we may repeatedly perform a small task. For example, you may want to continuously check /var/adm/utmp and report when a user logs in/out.

Bottom-halves are checked for execution upon every return from a system call, as you can see in arch/i386/kernel/entry.S. Take a look at kernel/softirq.c as well.



```
------------------------------------------
/*
 *      init_bh initializes a function as a handler, mark_bh marks
 *      it to be executed upon the next scout for bottom-halves,
 *      disable_bh uninitializes it.  Each time a bottom-half is run,
 *      it is removed from the queue, therefore we call mark_bh after
 *      each run of the registered function.
 */

#include <linux/kernel.h>
#include <linux/module.h>
#include <linux/sched.h>
#include <linux/interrupt.h>

#define EMPTY_BH      30

static void our_half(void *);

int
init_module()
{
        init_bh(EMPTY_BH, (void *) our_half);
        mark_bh(EMPTY_BH);

        return 0;
}

static void
our_half(void *null)
{
        /* insert code here... */

        mark_bh(EMPTY_BH);       /* mark to run again */
}

void
cleanup_module()
{
        disable_bh(EMPTY_BH);
}
------------------------------------------
```

How To Hack CyberTime Software

by Waphle/Managahtzul

In this article I will explain what Cybertime is, the coolest way to hack it, and how anyone can get the admin password in no time flat. Then I go into detail about some other hacks that also need to be fixed. And I finish with some nonsensical ravings of a teenager with girl problems.

Cybertime Software is the preferred time-restriction program used by Internet cafe's and other net clubs that offer access to T1 networks on suped up computers for a $5/hour fee. The reason it is so popular is that the site (www.cybertimesoftware.com) offers a fully operational download.

The software has two main parts: a server side to sell hours and monitor customer usage, and a client side that will lock a computer until a customer logs in. The installation requires that the client side computer have read/write access to the installation directory on the server. That translates to the client computer having access to 1) the password hash of cybertime and 2) the ability to run server programs from the client computer. I found the hash to be stored in the c:\ct5\lh global information.dbf. (C:\ct5 is default installation.) The hash is kinda imbedded at the end of the rather small file. (It contains the admin login name and password only.) I couldn't find a hash cruncher that could make heads or tales of it, so I did what any 2600 reader would do. I made my own. It took a few hours to understand how the algorithm was encrypting the passwords/accounts but the fact that it didn't add any random characters to the hash made it a lot easier. So here's the coding table for alpha numeric accounts and passwords. I didn't want to mess around with *all* the ascii possibilities. Compare the position of a hash character in the string so it will correlate to the character at left, i.e., password ABCDE = hash 6T2FG, clever, but obviously not enough.

Encryption Table for Master Admin Account/Password

A	6SZ~~~~m~maSZ~~
B	8T0++++B+BbT0++
C	<22____C_CVZ2__
D	,04FFFFvFvW04FF
E	/2]GGGGwGwX2]GG
F	[4(HHHHxHxY4(HH
G	:]~IIIIyIy)]~II
H	o[+JJJJ(J(^[+JJ
I	p~_KKKK&K&^~_KK
J	q+FLLLL%L%S+FLL
K	r_GMMMM£M£!_GMM
L	sFHaaaaNaNnFHaa
M	tGIbbbbObOUGIbb
N	zHJVVVVuVuAHJVV
O	1IKWWWWvWvDIKWW
P	3JLXXXXdXdEJLXX
Q	[KMYYYY5Y50KMYY
R	}La))))7)78La))
S	#Mb****9*9<Mb**
T	=aV^^^^>^>,aV^^
U	-bWS$$$.$./bWS$
V	cVX!!!!N!VX!!
W	fWYnnnn;n;:WYnn
X	gX)UUUU@U@oX)UU
Y	hY^AAAAPAPpY^AA
Z	i)^DDDDQDQq)^DD
1	K&£5555r5rS&£55
2	k^!6666S6Ss^!66
3	L%N7777s7sT%N77
4	l$n8888T8Tt$n88
5	M£O9999t9tZ£O99
6	m!U<<<<Z<Z>!U<<
7	aNu>>>>z>z0Nu>>
8	BnA,,,,0,01nA,,
9	bOc....1.12Oc..
0	j^SEEEEREERr^SEE

The best way to get CUSTOMER login names and passwords is to do a search for the backups (*.CTB) that store the passwords in cleartext. Or once the Admin password is snatched, use the customer server program to view the passwords. Note that all that was done to hack Cybertime so far was to download the program, read the manual, and use Notepad to look through all the files as the password was changed. The next part of the hack required the use of incontrol4 (www.wintoolbox.com). Incontrol is very useful for detecting trojans and stuff that like to do things sneaky without telling you (like adding a line to your autoexec.bat that formats your computer). Cybertime's server side has an annoying function that will only let you make about 240 transactions before the package expires. So I set out to find it. And, using incontrol, I found that it was making changes to two keys in registry:

A. HKEY_LOCAL_MACHINE\SOFTWARE\CTS\BDE_MODE

B. HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\WinBuild\BuildAdd

As I learned more about incontrol4 I got it to actively listen to the changes as I kept making transactions with a fictitious customer and I figured out (quite simply) the correlation between the key data and the remaining days had a pattern. So I once again made a coding table. Now on my computer the chart let me make up the "number" bXs for 999. That did let me make 999 saves to my fictitious customers. But when I tried to impress my buddies at "cyberhouse" by adding the extra saves to the software... it crashed and said the package had expired. So I am pretty sure that every installation creates a new coding table, but still, you can use the above method to just decode it each time.

Date tracking counter encryption table

	100	10	1's
9	b	X	s
8	B	w	S
7	a	W	r
6	o	v	R
5	M	V	q
4	l	C	Q
3	L	v	p
2	k	B	P
1	K	a	o
0	m	@	

A big N will mean negative.

Well, that about covers the elite hacks. The rest are pretty lame, but they are effective and if you're thinking about purchasing the software you should at least know of them.

The evaluation copy will alert you that you are using a demo copy every time you login. When this happens, stick in a CD that has an auto-run on it. The auto-run will play over the prompt and you can play whatever's on it. Another method is to login, click OK on the silly prompt, double click on the game to be played, then logout, login, and wait at the Message for the game to load. This will work on any game that takes a few seconds to load a CGI intro. If your cafe has the registered version of Cybertime, the demo warning will not appear. Most owners can't refuse the urge to put their own little message in its place.

The second way to defeat it is to login and (if running NT) logout of the computer and click cancel. This will get you into the computer, but all the useful shortcuts are gone.

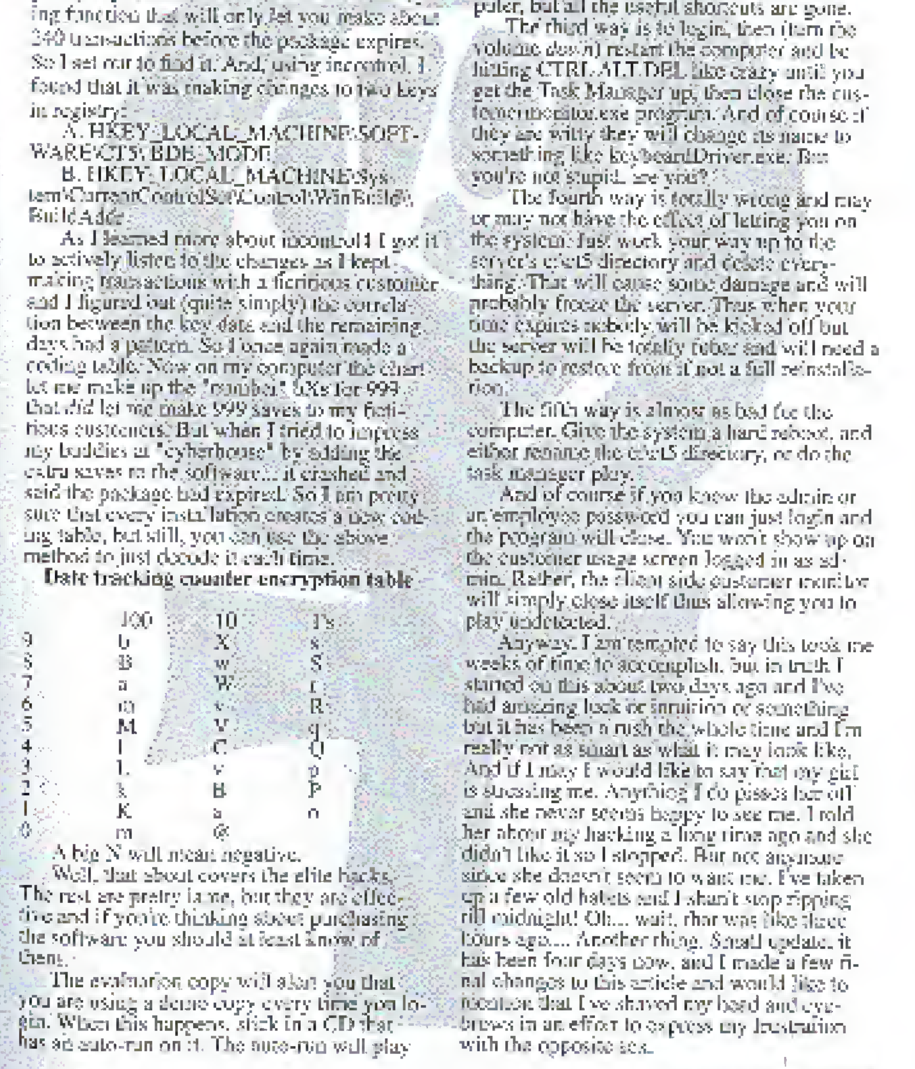
The third way is to login, then (turn the volume *down*) restart the computer and be hitting CTRL ALT DEL like crazy until you get the Task Manager up, then close the customermonitor.exe program. And of course if they are witty they will change its name to something like keyboardDriver.exe. But you're not stupid, are you?

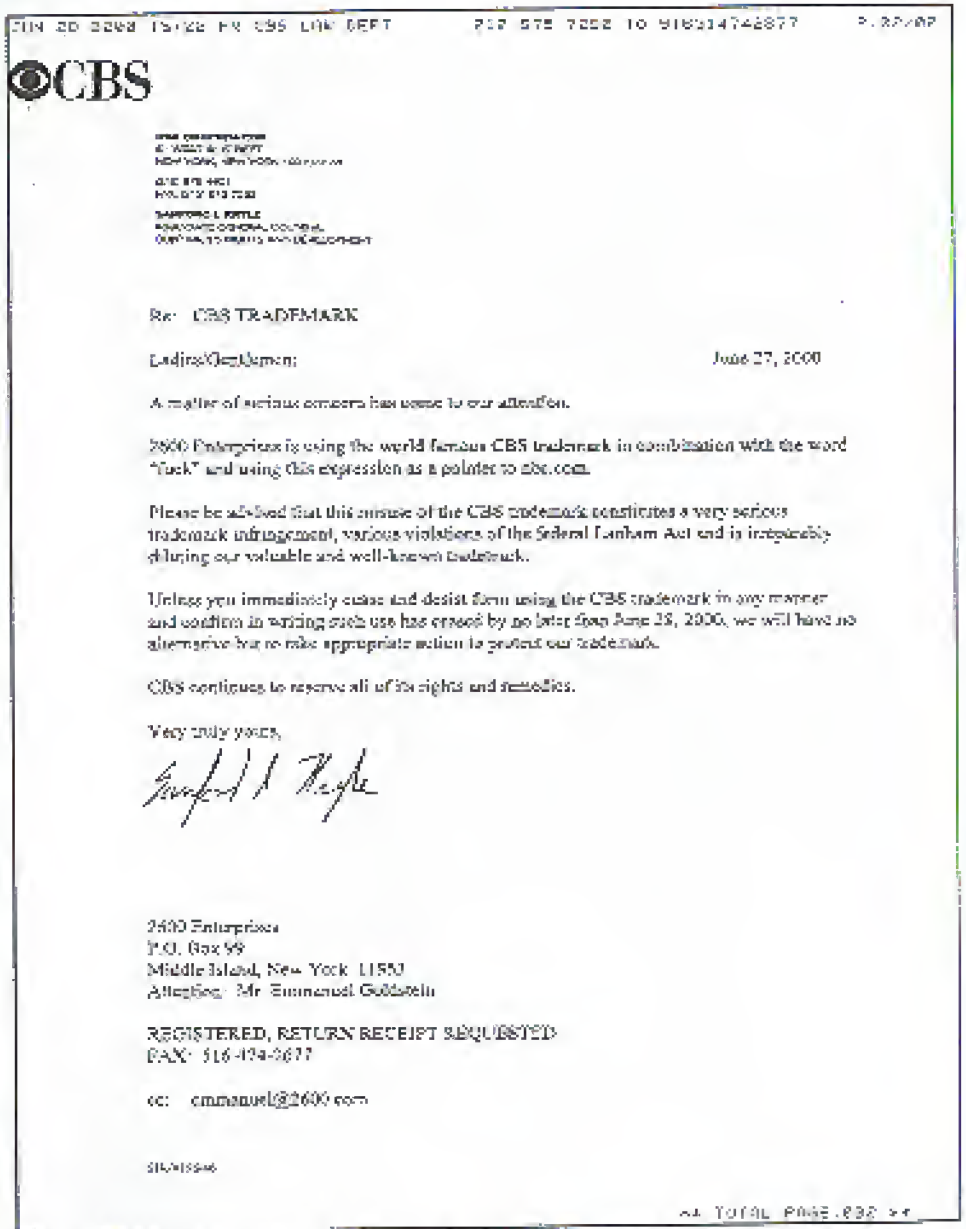
The fourth way is totally wrong and may or may not have the effect of letting you on the system. Just work your way up to the server's c:\ct5 directory and delete everything. That will cause some damage and will probably freeze the server. Thus when your time expires nobody will be kicked off but the server will be totally fubar and will need a backup to restore from if not a full reinstallation.

The fifth way is almost as bad for the computer. Give the system a hard reboot, and either rename the c:\ct5 directory, or do the task manager play.

And of course if you know the admin or an employee password you can just login and the program will close. You won't show up on the customer usage screen logged in as admin. Rather, the client side customer monitor will simply close itself thus allowing you to play undetected.

Anyway, I am tempted to say this took me weeks of time to accomplish, but in truth I started on this about two days ago and I've had amazing luck or intuition or something but it has been a rush the whole time and I'm really not as smart as what it may look like. And if I may I would like to say that my girl is stressing me. Anything I do pisses her off and she never seems happy to see me. I told her about my hacking a long time ago and she didn't like it so I stopped. But not anymore since she doesn't seem to want me. I've taken up a few old habits and I shan't stop ripping till midnight! Oh... wait, that was like three hours ago.... Another thing. Small update: it has been four days now, and I made a few final changes to this article and would like to mention that I've shaved my head and eyebrows in an effort to express my frustration with the opposite sex.





JUN 28 2000 15:22 FR CBS LAW DEPT 212 975 7292 TO 916314742877 P.02/02

CBS

CBS CORPORATION
51 WEST 52 STREET
NEW YORK, NEW YORK 10019-6188
(212) 975-4321
FAX (212) 975-7292
SANFORD I. [illegible]
ASSOCIATE GENERAL COUNSEL
CONTRACTS, RIGHTS AND DEVELOPMENT

Re: CBS TRADEMARK

Ladies/Gentlemen: June 27, 2000

A matter of serious concern has come to our attention.

2600 Enterprises is using the world famous CBS trademark in combination with the word "fuck" and using this expression as a pointer to cbs.com.

Please be advised that this misuse of the CBS trademark constitutes a very serious trademark infringement, various violations of the federal Lanham Act and is irreparably diluting our valuable and well-known trademark.

Unless you immediately cease and desist from using the CBS trademark in any manner and confirm in writing such use has ceased by no later than June 28, 2000, we will have no alternative but to take appropriate action to protect our trademark.

CBS continues to reserve all of its rights and remedies.

Very truly yours,

2600 Enterprises
P.O. Box 99
Middle Island, New York 11953
Attention: Mr. Emmanuel Goldstein

REGISTERED, RETURN RECEIPT REQUESTED
FAX: 516-474-2677

cc: emmanuel@2600.com

SIV/13946

** TOTAL PAGE.002 **

NEVER LET IT BE SAID THAT WE DON'T ADMIT WHEN WE'RE WRONG. IN THE SUMMER ISSUE WE ACTUALLY PRAISED CBS (EVEN THOUGH THEIR PARENT COMPANY VIACOM IS PART OF THE MPAA LAWSUIT). WE SAID THEY WEREN'T FREAKING OUT OVER WWW.FUCKCBS.COM LIKE NBC WAS OVER WWW.FUCKNBC.COM. WERE WE EVER WRONG. IT SEEMS THAT THEY HADN'T HEARD OF THE SITE UNTIL WE SAID THAT! WE FEEL BAD THAT SOMEONE BEAT US TO FUCKFOX AND FUCKABC SO, IN ORDER TO GET MORE CORPORATE LETTERHEAD WE'RE REGISTERING WWW.FUCKABCANDFUCKFOXTOO.COM. LET'S SEE IF ONE DOMAIN CAN GENERATE THREATS FROM TWO DIFFERENT CORPORATIONS.

Target Advertising!

by Hiemlich VonScootertraus the 53rd

World War II brought a whole new category of weaponry into the modern arsenal. While nuclear bombs were probably the most well known and feared of the weapons developed during WWII, a lesser known yet much more widespread implement of war came into its own around the same time as the war broke out. This weapon is propaganda.

We've all seen the draft posters featuring Rosie the riveter or a handsome youthful soldier sticking it to the Jerry. The Germans, and to a lesser extent, the Japanese both used propaganda to fuel their war machines as well. The only real difference between their propaganda and ours is that we won the war.

So while the war for our lands raged on in the skies, the seas, and on the ground, the war for our minds went on as a subtle undercurrent to the fighting outside. After the war, rifles and cannons were hung up, but the battle for our eyes and ears went on unabated. All throughout the 50's and 60's, the US and the USSR slugged it out through the height of the Cold War. This was not just a competition to find out who had the larger stockpiles of weapons, it was also a fight to see who could control the minds of their people most completely.

But when the Cold War ended, the propaganda wars ended too, right? Unfortunately, no. Today our minds are continually fucked by corporations using the same old techniques the government employed for so many years. However, instead of calling it propaganda, it's referred to as advertising and marketing. Companies battle for our thoughts more fiercely than any other battle in history. Every day we are subjected to over 500 separate advertisements. They're in the sky, on buildings, on the radio, in magazines, in movies, on TV, on our computer screens, they're even played over the phone while we're on hold.

Advertising is truly one of the greatest evils of our time. So what can you do about it? For starters, you must understand what advertisers think they know about you. To an advertising house, you are a number. You simply fall into various categories. You may be a gum-chewer, a video gamer, a nose picker, anything but a person. Advertising campaigns are built on the principle of throwing the largest possible number of messages at the largest possible concentration of a single group. This is why you always see beer commercials broadcast during sports games, and cereal commercials on Saturday morning. Advertising does not take into account the actions of the individual. People are like sheep: if you can convince the majority of them to come to you, the rest will follow the herd. (Interestingly enough, sheep are also the easiest animals to rape.)

Which brings up the most nefarious plot advertisers have devised. The guiding rule of Madison Avenue is "Get them while they're young." While the mainstream media has attributed this ideal to the cigarette industry, it is in fact a guiding light for the rest of the product making world as well. Children are very easy to control. With only a basic understanding of psychology, one can easily get inside the mind of a child. In fact, a great deal of modern child psychologists are employed by the advertising industry to help figure out just what it is that kids will want their parents to buy for them. Anyone who's ever been in Toys R Us knows exactly what happens when kids see a toy ad and decide they can't live without it.

So what can you do to slow the crushing tide of advertising propaganda? For starters, you can deface advertising whenever possible. There's no reason that a billboard or bus-stop-side ad should remain undefaced when the sign is on public land. Indeed, the cities belong to the people; we should be allowed to remove any unsightly ads if we so choose.

TOXIC SLUDGE IS GOOD FOR YOU!
LIES, DAMN LIES AND THE PUBLIC RELATIONS INDUSTRY
JOHN STAUBER AND SHELDON RAMPTON
INTRODUCTION BY MARK DOWIE

Another disturbing trend shows up at the movies. How many ads have you had to endure at the theater recently? Movie previews are all fine and dandy, but regular old ads an abomination. A new silent code needs to be installed: when ads are played before a movie, they must be heckled ala *Mystery Science Theater 3000*.

Finally, the world's largest purveyor of propaganda is by far the Coca Cola company. There is nary a city in the world which doesn't sell Coke at a corner shop. Coke is almost as recognizable a symbol as the Christian cross (an ancient symbol of the greatest work of propaganda ever: the Bible). Coke has single-handedly turned the advertising ideal of branding (imprinting your name in the customer's mind) to new heights. They sponsor everything! It's as if Coke wishes to insure that no fun is had on planet Earth without Coke being associated with said fun.

So keep your eyes and ears closed. Ignore propaganda in all its forms, especially government based - it's the most despicable form. When a government or company is able to think for you, they have won. And we shall never lose as long as we have a mute button on the TV.

An Introduction To Sprint ION

by The Prophet

Sprint Integrated On Demand Network (ION) is an integrated voice and data services network, which is available on a limited basis in the Denver, Kansas City, and Seattle areas (and coming to other cities soon). ION includes local and long distance calling, call waiting, caller ID, voicemail, and Internet service. As of this writing, there is only one service package available; it includes four telephone lines with unlimited local calling and a shared 750 minute long distance package, Internet service with two static IP addresses at up to 8 megabits per second (Mbps) downstream and 1Mbps upstream (although this varies depending on the quality of the local loop), voicemail, an Earthlink account with dial-up access and five e-mail user accounts, and a 3com Home Connect USB digital camera. The price for this service is $159 per month. Sprint also plans to offer a service aimed at residential subscribers, which will offer 1Mbps downstream and 128Kbps upstream, along with two telephone lines, for about $80 per month. Installation costs $300, and includes installation of Sprint's Integrated Services Hub (ISH), all necessary telephone wiring, and up to two new RJ-45 Ethernet jacks. To order Sprint ION, you must be in the service area and live in a single-family residence. You must also agree to a very broadly worded service contract, which gives Sprint the right to monitor all of your Internet usage, and sell the data in aggregate.

Physical Topology

There are three main components to the ION service: the Integrated Services Hub (ISH), a dry pair copper loop that Sprint leases from your local phone company, and Sprint's own equipment. ION service comes to you by way of a channelized ATM connection, ranging from 4-8Mbps downstream and 500Kbps-1Mbps upstream (depending on distance). There are three channels: One carries Internet data, one carries voice signaling data, and one carries voice data. The ATM loop runs over a copper loop with no dial tone, which is leased from your local phone company (an Incumbent Local Exchange Carrier or ILEC). The ILEC calls this kind of line "dry pair."

Your ISH is on one side of the ATM connection, and a Lucent 24-port DSLAM card is on the other side. The Lucent "Stinger" series DSLAM is located in Sprint's locked co-location cage, which is inside of the ILEC's central office (CO). Only authorized Sprint personnel and contractors can gain access to the co-location cage. Sprint maintains all of the equipment necessary to provide you with ION service, with the exception of the dry pair that is leased from your ILEC. If there is a problem with the dry pair, Sprint must contact the ILEC on your behalf; you cannot contact the ILEC directly.

Integrated Services Hub

The Integrated Services Hub (ISH) is a combination router and multiplexer, which you buy from Sprint as part of the installation. If you later move, re-installing the ISH is half price. My ISH is a large black box that mounts on the wall. It contains five RJ-11 jacks and two RJ-45 jacks. One of the RJ-11 jacks is used for the ATM connection, and the remaining four RJ-11 jacks are used for telephone lines. The RJ-11 and RJ-45 jacks are on cards, similar to line cards in a central office. On my ISH, there is room for seven additional cards, each of which can contain up to four phone lines or two RJ-45 jacks apiece. This means that a single ISH of this type can handle up to 32 telephone lines. The large black ISH design is likely to be installed primarily in small business environments. A smaller version of the ISH is available, which is designed for residential use. It is white, and does not have the space for expansion that the larger black ISH does. Otherwise, the two units are functionally identical.

The ATM drop connects to your ISH by way of an RJ-11 cable. The cabling is done by Sprint ION's installers, and runs between the ISH and the Network Interface Device (NID) on the side of your house. A separate 4 pair cable runs from the RJ-11 jacks on the ISH back to the NID, where each pair is connected to your home's inside telephone wiring. I run a crossover cable from one of the RJ-45 jacks on the ISH to my 10/100BaseT Ethernet switch; you can also plug a computer directly into the RJ-45 jack. The ISH operates at 10BaseT or 100BaseT speeds, in either full or half-duplex.

Sprint can remotely maintain your ISH, and has broad management features. Technicians can view the number of MAC addresses on your network, the number of active telephone calls, and more. Sprint also regularly updates the software in the ISH, transparent to the user.

Voice Routing

When you make a telephone call, your voice traffic is carried using Real Time Protocol (RTP), and signaling data is carried alongside it using Simple Gateway Control Protocol (SGCP). Both streams are converted to ATM-encapsulated IP packets at the ISH, and routed over the ATM loop through Sprint's ATM cloud. A separate ATM cloud covers each Metropolitan Service Area (MSA), for example, the Kansas City or Denver areas. At Sprint's central office, these packets are converted to regular channelized voice traffic plus SS7 data. This is accomplished using proprietary Telcordia (formerly Bellcore) software called Service Manager, which runs on HP 9000 series computers. Depending on the type of traffic (long distance or local, respectively), it is either routed to Sprint's long distance network or to the local ILEC tandem (usually a Nortel DMS250), except if a call is to another Sprint ION number. If the call is to another Sprint ION number, it remains entirely within the Sprint ION network, and is called an "on-net" call. On-net calls are always free, regardless of distance. This is because Sprint does not incur access charges in carrying them. This makes ION the first service where any call can be a local call. Because voice over IP over ATM is not efficient, Sprint is migrating to an end-to-end ATM solution for voice traffic. When on-demand video (which is presently being tested internally) is available, it will be carried as end-to-end ATM.

Data Routing and Performance

In order to use data service with Sprint ION, it is first necessary to register the MAC address of your network card. You do this at http://register.sprintbbd.com. Sprint keeps a static table of MAC registrations and you cannot register more than 10 different MAC addresses before someone has to manually clear the table. Sprint, unlike most DSL or cable providers, has no restrictions (subject to their Terms of Service) against running Internet servers, using network address translation (NAT) or other Internet connection sharing methods, or using PPTP, RAS, or IP tunneling services. Like voice traffic, data traffic is also carried as IP over ATM. All data traffic, regardless of origination, is routed to sprintlink.net in Kansas City. Since well connected private peers are almost exclusively used, latency is much less than at the public peering points. While Sprint claims maximum theoretical data performance of 8Mbps downstream and 1Mbps upstream, it must be recognized that this bandwidth is shared between your voice telephone lines and the data portion of the service. I am located one mile away from my central office and my loop operates at 6.4Mbps downstream, and 640Kbps upstream. As a practical matter, data transfer speeds are often limited by the speed of the site that you are connecting to. From http://www.gamesdomain.com, I can average 350K-400KB/s. I receive similar performance from other well connected sites such as http://[illegible].

Dashboard

Sprint offers a utility called Dashboard, which is an SSL page located at https://www.sdm.sprint.com. Ostensibly, this is branded "Sprint ION Control Center," but Sprint personnel always refer to the product as Dashboard. When you log onto Dashboard, you have access to localized Earthlink content, such as news and weather. If you need support with your Earthlink account, you can also receive it through the Dashboard. You can also leave technical support e-mail messages to Sprint ION staff. Finally, a video phone feature is included.

The most interesting part of Dashboard is Home Manager. Using Home Manager, you can control the behavior of call forwarding, anonymous call rejection, call waiting, and caller ID blocking from your PC. You can also change the ports on the ISH on which your telephones ring (allowing you to change which phones ring in what rooms with only a few mouse clicks). Finally, you can create additional accounts that are authorized to use Dashboard and control which functions that these accounts can perform.

In the future, Sprint plans to add additional features to Dashboard. You will be able to retrieve and play voicemail messages on your PC, order pay-per-view movies, and view the number of minutes remaining in your plan. You will also be able to view and pay your bill, and update billing information.

Ticketing Procedures

Customers who are experiencing difficulty with ION service call 1-877-806-4668. They are then connected to the Ion Solutions Center (INSC) in Atlanta, Georgia. This is the first level of support. The representatives there are trained to handle most routine customer support issues. They also serve as a filter to other groups within Sprint ION; customers are never allowed to talk to anyone outside of the INSC. If the trouble is beyond the scope of the INSC's abilities, they will open a trouble ticket, which is assigned a severity level and sent to the appropriate "fix agency." The fix agency will vary depending on the type of trouble.

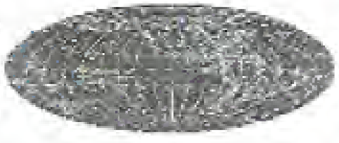
In general, problems with data connectivity are referred to the Internet Service Center (ISC) in Atlanta, and problems with voice connectivity are referred to the ISMC in Kansas City. If the problems are determined to be with the physical hardware, Broadband Local Network Operations (BLNO) is contacted. They deal with ILECs and the hardware in the co-location cages inside of CO's. If other equipment in the Sprint network has undergone a physical failure, the NTAC network operations center handles the problem. Because of all of the different organizations responsible for fixing problems with the network, it can sometimes take several days to get a problem resolved if multiple agencies are involved.

Telephone Numbers

The following are the telephone numbers used internally at Sprint to contact various fix agencies. Customers should not call these numbers directly; they will be referred back to the INSC (at 877-806-4668).

ISMC: 913-534-7200
BLNO: 877-602-2255
Dispatch (Earthlink): 800-356-5943
Dashboard PW Reset: 877-746-8456
Voicemail PW Reset: 877-282-6190

THE GEOSPATIAL REVOLUTION



by Silvio Manuel

This article serves to illustrate the explosion in Geographic Information Systems that has paralleled the growth of the IT world in general. It is a summary of 1) what a Geographic Information System (GIS) is, 2) the main software vendors involved in the GIS market; and 3) why it is important to you. This article is not a detailed explanation of GIS programming, nor does its scope encompass the intricate details of different GIS platforms. In short, this article's purpose is to provide the reader with a basic understanding of GIS without exploring the subject in intricate detail.

Geographic Information Systems finds its roots in two disciplines, Geography and Statistical Analyses. The advent of computing, and more accurately, powerful microcomputing allowed the development of GIS systems. The core to any GIS is the ability to combine tabular data with an exact spatial location. A ready example can be found in census data, where enormous amounts of detailed information are located. By implementing this data into a GIS, the entire database can be queried, not only by database fields, but also by spatial requirements. This is equivalent to looking at a paper map of the United States which is filled with thumbtacks. Each thumbtack has a piece of paper attached, detailing the information about that location. By using a GIS complex, analyses can be performed on a location.

The uses of a GIS are limited only by the ability of its owner and the data available. It has become popular in everything from city planning to ecological conservation. At the heart of the system lies a topological model to which the data is pinned. The data file, which is almost always vector-oriented (if it is not vector then some means must be available to emulate this), is populated with a database of records. The spatial pieces of the data, which resemble its real world counterpart, are comprised of points, lines, and polygons. Since the file has topology, every line has a "right" and a "left," and every polygon has an "in" and an "out." This is how each database record is linked to its spatial coordinates. The most visible example of this is your local Emergency 911 system.

Most E911 systems across the country are now based on a GIS. This is the reason all rural routes were given E911 addresses, so that they could be more easily located (and this also makes them more easily assimilated into the GIS database). When you tell the E911 operator your address, (and I don't even think it's necessary to tell them anymore), it is fed through the GIS. The address is analyzed (it is either a left or a right address), then the appropriate record in the GIS is found using this code. Once the record is located, GIS utilities like ESRI's Network Analyst can determine the quickest route from several different locations, taking into consideration traffic flow, traffic congestion, and any other variables for which data is available. This is a simple example, and I have seen much more complex uses. What makes this a viable system is its a) cheapness (most commercial GIS software packages are relatively cheap), b) its ease of use (although earlier versions of GIS software could be extremely complex, this has changed in recent years), and most importantly, c) the ease with which it can be customized.

Several GIS packages are available commercially, but the most popular are MapInfo, MGE, ArcView, GeoMedia, and ArcInfo. MGE is based on the Microstation CAD engine, developed by Bentley Systems and Intergraph. ArcView and ArcInfo are both distributed by Environmental Systems Research Institute, commonly called ESRI. In the past Intergraph's packages dominated the GIS market but the last five years have seen ESRI rise to almost total dominance. This lead has been due to the company's devotion to distributing its software to educational institutions at large discounts, thus creating a trained workforce in college graduates, and to its scriptability. ArcView has its own scripting language, Avenue, that is simple but useful. Thousands of programs for specific tasks are easy to find on the Internet or from ESRI themselves. If a program is not available then one can be produced at little or no cost. This means that anyone can purchase the basic ArcView package and then tailor it to their specific needs.

So, why is any of this important? And how does it affect you? Anyone with even a little imagination can see how a system that can integrate and analyze huge databases with spatial data to create targeted, specific results in the form of maps, graphics, projections, etc. can be misused. And it is.

Some companies deal in this information. The spatial data is cheap, well, it's actually free. An almost limitless amount of geographic data is available from the United States Geological Survey, Terraserver, and other such sites. This data is being collected by some companies, who then assimilate the spatial information with massive databases compiled from grocery stores, mailing lists, credit reports, census data, and public records. This information is then sold to groups who use it in conjuction with a GIS to determine everything from lending qualifications to high crime areas. To 99.9 percent of the population, this goes on without their awareness or consent. If you apply for anything from health insurance to a loan, a company possessing such a database can reference your info and study where you live, what you eat, what you buy, and with a little guesswork, why you buy it. To many readers of 2600 this isn't a new idea, and to others it may seem a "conspiracy theory" or paranoid self-delusion. Yet it is an absolute reality.

For a detailed description of such practices, check out:

"Protecting Personal Privacy in Using Geographic Information Systems," *Photogrammetric Engineering and Remote Sensing*, Vol. 60, No. 9, September '94 pp. 1083-1095 ;

"We Know Who You Are and We Know Where You Live: The Instrumental Rationality of Geodemographic Systems," Jon Goss, Dept of Geography, Univ. of Hawaii.

The bottom line is that very soon in the future these systems will be an everyday part of our lives, with the possibility existing for them to be used or abused. Thus, it is necessary to have at least a basic understanding of them, how they are used, and how they affect you. This article has skimmed over a great deal, but hopefully will provide answers to the above questions. So keep an eye out, because someone really is watching you, and it ain't that guardian angel you keep talking about!

Anomaly Detection Systems

by Thuull

In order to talk about detection systems, we must first explore the intent behind what detection is all about. The whole idea is to identify attacks against your network, primarily to determine whether or not an attack may have been successful and to get a handle on what is currently being done "on the other side of the fence," so to speak.

Intrusion Detection systems have primarily been compartmentalized into four distinct camps, which in themselves are defined by a combination of two factors. First, a system can be "Active" or it can be "Passive." Second, it can be "Host Based" or "Network Based." So, when combined, you can have an intrusion detection system that is "Active/Host Based," "Passive/Host Based," "Active/Network Based," or "Passive/Network Based." There are obviously other ways that IDS systems can be categorized, but this paradigm set forth by Internet Security Systems pretty much covers all the bases.

In order to be classified as an "Active" IDS, the system must be capable of real-time (or near real-time) response to an identified incoming attack, such as updating firewall rules based on the attack, or notifying a command console of the activity immediately after it occurs. "Passive" systems generally record the activity and store it for easy reference at a later date. "Host Based" systems are exactly that; they reside on the individual hosts that are being targeted. "Network Based" systems sit somewhere on the network between the attacker and the target, and spy on the traffic as it flows by, looking for attacks. Generally, network based systems reside either in a demilitarized zone (DMZ), between a network's firewall and their upstream provider, between the network's firewall and the rest of the internal network, or any combination of these three.

Now, let's talk a little bit about trends. Since the inception of intrusion detection systems as we know them today, they have generally been based around the concept of "attack signatures." That is, every attack has a signature that distinguishes itself from other normal network traffic and from other attacks. This is done very similarly to the way that most popular virus scanners are designed. The system scans all the traffic, and when it sees a pattern that matches that of a known attack, it does whatever it was set up to do (page an admin, update firewall rules, notify a console, etc.).

An oft unrecognized means of accomplishing intrusion detection is "Anomaly Detection." With an anomaly detection system, traffic that normally can be found on the network is ignored, and bits of traffic that are not normally seen are highlighted and brought to the network owner's attention. This has distinct advantages, as outlined below.

We all know that there is no such thing as a "secure" system. Every machine that is attached to the Internet today can have its security defeated. What keeps this from happening in most cases is that the vulnerabilities that are on the systems have not yet been found. But they're there, you can bet on it. So, what happens when a new vulnerability is found? The individual that found it will likely create some exploit code for it, to take advantage of the vulnerability. This code is then shared with friends, or kept to oneself for a certain period of time. Eventually, it will probably end up in the hands of the security community as a whole, and a fix for the vulnerability will be coded. Now, between the time that the exploit is coded, and the fix is coded, what good are intrusion detection systems based on attack signature? None, whatsoever. Simply because of the fact that in order to be able to define a signature that identifies a criminate attack, one must know what that attack "looks like" as it crosses the wire, or finds itself on its target system.

What I plan to set forth with this article is an alternate means of "visualizing" security on your network, be it four Linux machines sitting behind a dual channel ISDN, or the largest banking network in the world.

Let's make some assumptions:

A. You cannot keep someone who wants access to your network from obtaining access, short of unplugging the machine.

B. You cannot stop someone from wanting to gain access to your network.

C. You have limited resources to accomplish your security (don't we all?).

With these assumptions in mind, what can you do? Well, you can throw manpower and resources at solving the problem - purchase clustered firewalls, intrusion detection systems, secure all of the machines in the network, etc. But, what is the best that you can really hope to accomplish?

The best you can really do is make it difficult enough for the attacker to get in so that it takes him more time to do so than he intended. Second, you can identify the initial scanning that must take place in order to determine what services exist on your network that may be vulnerable. And, third, you can take actions, either aggressive or passive, to ensure that the traffic no longer continues to be able to access the machines that may be vulnerable.

How can you do this? How can you identify all traffic that may be questionable, even exploits that were coded yesterday? Anomaly Detection.

An extremely effective Anomaly Detection system can be built on any Linux platform with simple freeware tools and a little modification. These tools consist of ipchains/ipfwadm, portsentry, logcheck, gnumeric, and an e-mail address. Here's how the system works.

On every system, ipchains/ipfwadm is set up to log all traffic going to ports that are not listeners. If it's a webserver and you use ssh, have ipchains log every packet that goes to any port other than 22/tcp or 80/tcp. Modify portsentry to execute logcheck anytime that portsentry trips. Use portsentry -aclp. Modify logcheck to e-mail you any unusual activity that appears in the logs to your e-mail address. Use gnumeric, or any other spreadsheet that you like, to maintain a record of every rogue packet on each machine. Maintain ip address, date and time of the activity, ports involved (including source port), dns resolution of the offending ip address (if available), and contact information re: the owners of those ip addresses.

With this system in place, you will see every packet that enters your network that does not belong on your network. Every packet. Face it, for an attacker to be able to compromise your system, he must know what services are running, what OS's you use, etc. He must do some preliminary checking to determine what is on your network. Slow him down, give yourself the ability to see it happening, and give yourself some time to respond. The response, of course, I leave up to you.

Hunting The Paper Carnivore

by BrotherBen

I am sure most *2600* readers out there have heard about Carnivore. If not, I advise all parties interested in privacy and Internet security to do a quick search on "carnivore FBI" and do a little a reading. Carnivore (originally called "Omnivore") is a system designed to analyze huge amounts of email traffic and extract any mail sent to or from individuals for whom wiretapping warrants have been issued. By law the device should not be used to indiscriminately scan all public Internet communications. Naturally that is against the law and at least on paper neither Carnivore, traditional wiretaps, nor the "mythical" ECHELON can be used against US citizens without a court order. But more on that later.

I have been informed by sources close to the FBI (think Infrastructure) that Carnivore is nothing more than a glorified sniffer. The media is describing the device as an email scanner that collects all traffic received by targeted ISPs and "selects" messages sent by individuals for whom the FBI has received wiretapping warrants. There are many ways this could be accomplished, such as installing a script on the mail gateway that greps for certain messages and sends them on to an analysis machine, but in fact the deadly "Carnivore" simply sniffs all traffic at strategic bottlenecks on the ISP to perform its mission. There are literally a dozen different scenarios I could envision for sniffing an ISP's mail gateway, but the end result is the same: Carnivore sniffs all port 25 traffic, collects the data, examines the mail headers for target senders and recipients, and finally archives those messages. An agent shows up daily at the ISP to collect a floppy/zip/whatever archive of the messages (interestingly enough, the PC housing the Carnivore software (script?) is reportedly locked in a cage 24-7). Note that Carnivore could collect traffic from any port, but almost all of the printed quotes from FBI officials refer to the device as an email scanner. However, the current state of wiretapping laws in the USA may allow sniffing of just about any type of traffic, including web surfing. In fact, I am sure the FBI would begin collecting html traffic if a target were using Hotmail or Deja as a mail service.

The media has hyped Carnivore heavily in recent months due to privacy issues raised by certain groups (such as the ACLU and EPIC), but the concept of Carnivore is nothing new. In fact, the ACLU is far too late to play the role of alarmist, as the FBI has been conducting limited Internet surveillance operations without Carnivore for years - and getting similar results. What has raised media interest lately is the fact that at least one ISP has been ordered to allow the FBI to scan their e-mail traffic on a daily basis. The problem here is that the FBI presumably collects *all* TCP/IP traffic and discards that information not pertinent to the current mission. In theory then, the FBI must at least temporarily "listen in" on *all* e-mail sent to a given ISP in order to track one or two suspects. Likewise, depending on the configuration of the scanner, the FBI could be receiving all TCP/IP traffic routed to that subnet (see above). We are left to trust that the FBI will only use the information it needs to accomplish its mission, and that these "needs" are modest and lawful in scope.

The point of this article is not to present a paranoid rant about yet another invasion of our privacy - we have all experienced our share of government ignorance, oppression, lies, etc. In fact the Carnivore device itself is quite mundane, assuming it doesn't end up in a role similar to ECHELON, in which private communications are subjected to a logic engine that evaluates messages for threat conditions. The capability is there, of course, and once again we have to trust the establishment to control itself - something our government was never designed to do. In the FBI's defense, I have been told that there are oversight committees designed to prevent abuses of power, but technology issues are very difficult to oversee because members of oversight committees are not always technically proficient enough to understand the actual threats involved. We see similar problems occurring with the depositions in the MPAA/2600 case.

The critical issue with Carnivore is the level of access initially granted to the FBI for operations. *All* traffic could likely be collected and examined at the whim (or misconfiguration) of an agent. Current wiretapping laws are simply incapable of adequately dealing with email, because the amount of traffic and technology concerns differ greatly from the POTS systems of the past decades (in fact, one could argue that modern telephone systems have outgrown traditional wiretapping statutes). Wiretapping laws have been modified over the past few years, but in fact a real understanding of global, switched data communications is still in development. The recent court order concerning ISPs and Carnivore proves this perfectly - we now have tap and trace regulations being applied to a medium in which "bad" communications are tightly interwoven with "good" ones, and the FBI is left picking through our lives in search of a few bad apples. I hope this trend changes soon but patience alone will not institute such a change.

Naturally I understand that cryptography appears to be a panacea for the Carnivores amongst us. Even though I advise all serious privacy advocates to use cryptography whenever necessary, viewing cryptography as a final solution is flawed for two reasons. For one, it is not enough to reactively avoid bad legislation by using "loopholes" such as cryptography. We cannot assume that our current algorithms are indecipherable, or that cryptography will soon become mainstream. We must act to stop the trends in legislation by proactively voicing our discontent. Secondly, if the powers of the FBI are circumvented by our regular application of strong crypto, we may see another push to increase surveillance powers, such as registering private keys - probably in the name of stopping terrorism. The end result will be the increased control over communication lines by various agencies. As stated earlier, the use of public mail services such as Hotmail and chat protocols like IRC will certainly prompt the FBI to monitor other types of IP traffic.

I have never seen the government back down from a fight just because they were outsmarted (arguably, prohibition may be an exception to this). If we allow broad powers of search and seizure to exist, I seriously doubt that overt secrecy will act as anything more than a speed bump for our watchmen. The ultra-paranoid will always have a "solution" to problems such as Carnivore. SSH connections to remote systems running sendmail, dedicated, encrypted dial-up connections, and other VPN solutions all come to mind. Though using such methods is advisable, it is comparable to the tuna out-swimming the shark in the belly of the whale. The greater issue must be addressed.

The fact that exporting 128 bit encryption from the USA is viewed as a felonious offense should tell us how seriously our government misunderstands and over-legislates technology. We must normalize and distribute strong cryptographic systems, while simultaneously restricting the power of governmental institutions to control and prohibit technology. One cannot occur before the other.

VIA FACSIMILE: (631) 474-2577 (2 pgs.)

Debra Rudnick, Director
Theatrical Feature
Clearances and Permissions

Friday, July 07, 2000

Permissions
2600 Hacker Quarterly
7 Strong's Lane
Setauket, NY 11733
Bus: (631) 751-2600

WARNER BROS.

Production Clearance &
Permissions Department
4000 W. Olive, Suite 300
Burbank, CA 91522
818-977-2232
Fax: (818) 977-2238

Re: "Swordfish"

To Whom It May Concern:

Warner Bros. respectfully requests permission to use "2600 The Hacker Quarterly Magazine" as background setdressing/prop, in, and in connection with, our feature motion picture, currently entitled "Swordfish" (the "Picture"), starring John Travolta, and in connection with the distribution, exhibition, advertising and other exploitation of the Picture, by Warner Bros., its assignees and licensees, in all media whether now known or hereafter devised, in perpetuity throughout the world.

You understand and agree that Warner Bros. owns all rights in and to the Picture, and that we will be the primary worldwide distributor of the Picture, and that you will make no claims or demands based upon the above mentioned use. You represent and warrant that you are the owner, or the authorized representative of the owner, of the rights herein granted, are authorized to execute this letter of consent and that no third party permissions are required. You are granting this consent for no compensation, but you understand that Warner Bros. may rely on this consent if it elects to include the above material in the Picture. Neither this letter, nor the request for this letter, is intended to diminish Warner Bros.' right to use the material if and to the extent it would otherwise be permitted to do so by applicable laws.

Should you favor us with your consent, please indicate so by signing in the space provided below and faxing back to me at (818) 977-2238. If you have any questions or comments please feel free to call me at (818) 977-2152. Thank you for your courtesy and consideration in this matter where time is of the essence.

ACCEPTED AND AGREED:

Warner Bros., a division of Time Warner
Entertainment Company, L.P.

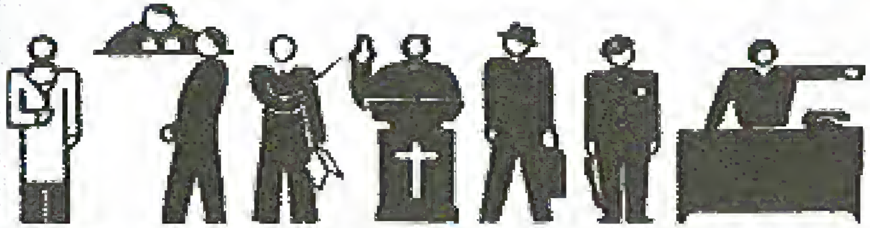
By: Debra Rudnick
Its: Authorized Representative

____
Name:

____
Title:

HOW'S THIS FOR NERVE? ON THE SAME LETTERHEAD AS THE COMPANY SUING US, THEY ASK FOR PERMISSION TO USE US FOR THEIR PROFIT. IT'S AMAZING HOW EVEN WHEN THEY'RE ASKING FOR A FAVOR THEY SOUND THREATENING! CAN YOU SAY WWW.FUCKWARNERBROTHERS.COM?

The Making of a Pseudo-Felon



by Brent Ranney

"I'm bored and depressed. I think I'll hack extenders for seven days, 24 hours a day. It's relatively harmless isn't it?"

At the age of 19, home from college, around the time of Thanksgiving 1993, I used a 386 computer, a special computer program, and a 2400bps modem to conduct hacking activity on midwest based LDDS Metromedia Communications - to obtain phone access codes through its service. In other words, I tried to cheat the telephone company.

In the middle of the night, I took a printout of access numbers the computer program generated and strolled over to a pay phone. I tested every access code. They all failed to work despite the computer program logging them as valid with a carrier signal.

When I returned to school, everything appeared normal. I was oblivious to the fact that a federal search warrant had been obtained to search my dorm room.

My friend and I were unaware of anything amiss when we entered our dorm building on an early winter evening. An anonymous student had tipped me off earlier in the parking lot that the school was considering me as a suspect for internal PBX abuse. I was not involved and knew nothing about it.

Before we entered the elevator to reach our floor, a student bellowed, "There's FBI agents running around on the 3rd floor!"

"That's our floor," I thought. "It must be drugs or something." I felt bad for whoever was getting arrested. Though feeling uneasy, I garnered some comfort in thinking it probably had nothing to do with me.

A pudgy man, his face almost blushing, was standing in front of my door conspicuously. The guy greeting me outside my dorm room happened to be the area manager of security for the local telephone company.

"Are you Brent?" he queried.

"Yesss," I said.

The phone cop turned around to face the door. He knocked two or three times. Immediately the door flew open and the barrels of small hand guns were pointed at me, wielded by men dressed in what you might call "land warrior nerd" attire. They were wearing telemarketer headsets and I heard the cracking of walkie-talkies.

I don't remember the specifics. All I know is that I was facing the other way, my hands against the wall up above my head. "What is this?" I asked.

They frisked me and my friend. "Do you have any weapons? Any knives? Guns?"

"No," I said, flabbergasted. On cue, an agent flashed his ID. It wasn't the FBI after all. It was the Secret Service.

I was shocked. Everything seemed to go in slow motion. I didn't feel like it was really happening. I was so nervous.

I asked for a lawyer. A couple of hours later, I found myself in an empty holding cell, after submitting to fingerprints, pictures, and idle chit-chat.

I had a friend, whose father was on duty as a cop the night when I came into the police station. "He looked like a stereotypical hacker," his father later told him. Apparently the man had seen a lot of hackers coming through the station (small as the town was) and he could spot them immediately.

Before I was left alone in the cell to lament my sins, another cop stayed behind and eyeballed me for a long minute. His look shot the message, "You're going to get it bad boy, and you are a bad boy, no matter what you think."

I signed a waiver for release, relinquishing some of my rights. I was released from police custody and returned to my dorm, a new man, stripped of all my electronic possessions. They had taken every computer-related article I had, every disk, every issue of *2600*. A year later, after my conviction, everything was returned, mostly broken. I just wish they hadn't destroyed the computer artwork I painstakingly created.

I withdrew from the school. "I hope you get away with it," my political science professor told me as I bid him farewell. "I hate the phone company," he added.

I met with the Secret Service agent again at a later date. Whenever I met the agent, the phone cop was with him - always present, under some shadowy pretense, like cancer-man from *The X Files*. I was encouraged, implicitly pressured, to reveal information on other people who committed crimes. I told them about real criminals I was aware of - people who were profiting from fraud.

In these closed door sessions, I admitted illegally obtaining the access codes and divulged every detail about the crime. Prior to my actual arrest, the area manager of security for the local telephone company contacted my mother and promised I would not be arrested or prosecuted, with the understanding that they just wanted me to stop. He told her I was responsible for $100,000 in damages. Unfortunately, she believed his white lie. He told her that if she didn't cooperate by disclosing my whereabouts, she would be an accessory to the crime.

Regardless of what was promised, I openly confessed to involvement unknowing of the unscrupulous tactics employed on my mother. A year later, I plead guilty to "possession of access codes with intent to defraud." I was sentenced to three years probation, fined $500, and ordered to participate in a a halfway house program for two months. Throughout my probation, I was tested for drugs. I had no drug history. What I did possess was long hair and a penchant for black clothing.

My offense is a felony for one reason and one reason only: the access codes could be used to call out to any state. Because of this interstate characteristic it is federal and therefore a felony charge. No losses were reported by any of the respective long distance companies I had tampered with, although the local company claimed a loss of about $17 to $30 in administrative fees. The judge and prosecution rationalized that taxpayers are indirectly victimized because of the cost related to investigations and prosecution of "major" cases such as mine.

I don't envy Kevin Mitnick for the ordeal he's endured with the government. I think of myself as lucky to have never spent a day in jail. If I had, I don't think I would have emerged a survivor. Quite honestly, I probably wouldn't be here today.

I don't think this mark on my record, this felony, reflects with much accuracy what kind of person I am, or what kind of employee I am. Many youths do stupid things which aren't necessarily injurious to anyone. Before Steve Wozniak and Steve Jobs co-founded Apple Computer, they "cheated" the phone company with a device called a "blue box" while in college at Berkeley, CA. Didn't they turn into quasi-responsible multimillionaires?

"They didn't get caught," a landlord said to me, whose rental operation routinely turned away convicted felons per police sponsored programs. Is this to be the scale in which we judge the severity of a crime? Simply speaking: "Don't get caught"?

There's no distinction today between a crime of violence and a recreational hacker. I don't expect there ever will be. How do you explain the proverbial Scarlet Letter to the uninformed public who thinks hackers like Kevin Mitnick are diabolic monsters?

Seven years later, I don't justify what I did back in '93. But society shouldn't exaggerate the impact of it either. The interests of the multi million dollar corporations have been protected, rest assured. Kevin Mitnick was silenced and before him so were many lesser-known hackers.

The branding is done, it's over. No appeals, no expunging. I am a convicted felon for life.

Are we to be made as examples, to sway public fear and distrust? Is this the result of manufactured propaganda to serve corporate interest? Should the minor aggravation of a corporation result in a lifetime felony conviction for a college kid?

I'm not hiding anything and I accept responsibility for something I should have never done for the sake of curiosity to make a few free phone calls.

Kevin Mitnick is, dare I say, an astute genius, but not a criminal mastermind. I was psychologically evaluated by the government and labeled off-the-record as not having "criminal thinking patterns." I've always considered myself an ethical person despite Ma Bell groupies who consider one guy with a few access codes to be of critical importance to the subversion of a nation.

Not abiding contemporary law has disproportionate consequences depending on whether or not the violation of the law involves life and limb or involves property. If you are thinking about tinkering with the phone company or other mega-corporations, think twice. Then consider beating your wife instead. By example of length of sentences served, this act is more acceptable to our society.

But, God forbid, "Don't get caught" beating your wife while in possession of a red box.

Afterthoughts

Since my conviction in the early 90's, I've ceased participating in any hacking activity - anything that might be construed as illegal. Frankly, I absolutely shudder at the thought. I don't keep myself privy to the latest hacking tools. I flee from gray areas of computer activity. I am 100 percent dedicated to a philosophy of anti-hacking. Call it fear, call it cowardice, but I capitulate with tyranny when it threatens my well-being. Paranoia is now a part of my everyday life.

I wasn't always that way. I use to stand up for myself. But the futility of raising arms against a million to one odds is not my cup of tea. But there are others, more courageous than me, who face these odds every day. You may know them: Bernie S., Kevin Mitnick, the staff of *2600*, and nameless others in America and in third world countries.

By writing this article, authoring it with my real name, I fear I'm jeopardizing my well-being. Without any prodding of our imagination, we can assume the Secret Service peruses *2600*. And if the SS thinks I've somehow resurfaced as a threat, they might conceivably pay me a visit. Like Bernie S., they might want to check my wiring.

I don't have a vendetta - I'm just telling a story and offering an opinion. I haven't voiced my disapproval in a domain name like *2600*. But I wonder, how is writing an opinionated article any different?

To the credit of law enforcement and in particular the probation department, I was treated humanely. I'm not going to judge these people. They generally respected me and I respect them. I do think they're part of a larger problem - a preoccupation with power, an aristocracy that pulls the government strings to protect Corporate America. (That's where these laws directed at hackers come from.) Perhaps this threatens our rights of freedom more than any hacker.

Flaws In Outsourced ECommerce Systems

by Dean Swift

I have been asked to write about flaws in ECommerce systems, in particular, systems for which I have written my shopping basket software. The general trend that I have discovered is that any web site that has third party credit card processing may be subject to a particular class of implementation flaw. I discovered this accidentally when interfacing my software to third party credit card processing software.

Few people write interfaces for ECommerce systems because numerous solutions have been written already. While it's productive to re-use existing software, potential flaws in a system are left unchecked. A flawed system can become popular because new users may assume that previous users were satisfied with criteria such as security.

I had written a shopping basket to the exact requirements of a clothing web site. One of the requirements was that the existing workflow (FTPing web pages) could continue. Another requirement was that the existing search engine listing could be maintained or improved. Another requirement was that any changes would preserve the level of compatibility. A further requirement was that it should be cheap to host. I was unable to find prior art which met the requirements, so I proceeded to write the software to specification.

This was the first version of MTECS (TM) - the Multiple Tier ECommerce System. The system is encapsulated into a number of stages or tiers. Unlike many layered systems, all of the tiers described are presented to the end user as web pages. Each tier can be hosted on a different web server or outsourced to a different party. MTECS Tier 1 is an optional program. It transparently modifies the web site to propagate a session key in the absence of cookie functionality in the web client.

MTECS Tier 2 is the shopping basket; a construct to allow more than one type of product to be accumulated before purchase. It was intended that further tiers would be added for payment, although Tier 2 functions as a stand alone program using the "Print 'N' Post" (TM) ordering system.

After architecting and implementing this solution, the customer decided not to deploy the software, which left me with software surplus to requirements. I was determined to use the software and it was re-purposed for digital books (http://www.great-books.com/), hydroponics (http://www.esoterichydroponics.com/), seeds (http://www.pukkaseeds.com/), power tools (http://www.huntertools.com/), my personal web site (http://www.gandalf.user.xirium.com/), and other web sites.

Each web site required the software to be adapted or required utility software. Fortunately, the requirements were not so demanding that other software would have been suitable. More fortunately, the initial web sites did not require credit card processing and depended on the standalone "Print 'N' Post" (TM) ordering system, which is more affordable and low in risk.

This changed after the success of Esoteric Hydroponics (http://www.esoterichydroponics.com/). After adding MTECS Tier 2, without credit card processing, return on investment for the entire web site occurred within two months. (It must be stated that the web site was fairly active with 44000 hits per month before the ECommerce software was added. The web site is fairly large and the URL of the web site is advertised in ongoing, targeted, print media advertising campaign. Additionally, the web site is distributed to potential customers as a platform independent CDROM.)

Esoteric wanted to add credit card processing to obtain more revenue and to keep ahead of competitors. A successful system would also be ported to Pukka Seeds (http://www.pukkaseeds.com/) and Hunter Tools (http://www.hunter-tools.com/). We evaluated the cost of processing credit card transactions and soon discovered that for small volumes, it would be cheaper, easier, and more secure to outsource.

Obviously, it was sensible to choose a company with established procedures and it was desirable to choose a company with low charges. There was also the stated requirement that the company should be based in the same country. This would reduce risk, simplify payment and minimize potential problems and associated cost. The market leader in the UK, NetBanx, was immediately eliminated, due to excessive charges and direct experience with the company.

We agreed upon WorldPay PLC (http://www.worldpay.com/), due to perceived technical competence and low initial costs. I was required to interface my software to WorldPay immediately. WorldPay has a 24 hour sign up process, although delays were encountered. WorldPay reduces costs by leveraging bank authentication processes and requires that signatures of representatives are confirmed by a bank. This requires a meeting with your bank manager and additional paperwork before WorldPay approval. WorldPay also requires a Direct Debit to be established before approval, presumably to ensure continued payment for service.

WorldPay also performs their own due diligence, at cost to the customer. This means that an organization failing this process does not get a full refund. Fortunately, some of the administration can be processed while web site development occurs. Two weeks later, after much paperwork and two days of programming and testing, it was done. Unfortunately, the software did not accurately reflect the business rules: haggling.

Esoteric Hydroponics allows discounts (on large volume purchases only). Of course, this would have to be provided securely so that it would not be open to abuse. I began writing a passworded utility to allow the insertion of a negative price, although this, quite sensibly, was not accepted by WorldPay. Then I considered writing a utility to dump the existing catalogue as a web page that would allow prices to be changed. This would sidestep the fixed pricing restriction of the shopping basket.

MTECS Tier 2 (the shopping basket) already has a utility to dump catalogues as HTML. After the catalogue has been uploaded, a CGI script can return a section or all of the catalogue as a web page. This can be modified and inserted into the web site as required. All that was required was an additional format for the output.

Unfortunately, this would be a *massive* security flaw. If the output was obtained, it would allow anyone to purchase anything at any price. With trivial modification, it would also be possible to order nonexistent items or items with subtle changes in description. This remains a problem because anyone with sufficient information and expertise may be able to implement such an attack.

Fortunately, Esoteric is already alert to such practice. I had demonstrated how easy it is to change prices with "Print 'N' Post" (TM). This facility is little more than a construct to ensure a legible order is received by snail mail. If someone accidentally or maliciously modifies the products and prices when placing an order by mail, it makes little difference whether the order is written or printed. Obviously, it requires more skill and effort to maliciously modify a web page, but this shows that computer output should not be trusted.

This left the matter of third party credit card processing. It is hard to obtain specific details from WorldPay. Indeed, I was unaware of some of the best technical features when WorldPay was selected. Nevertheless, with a growing client base, it is only a matter of time before such an attack would be attempted on a successful web site such as Esoteric Hydroponics. I immediately informed the client of the implications of the security flaw.

"That can't be right: we use the same system as VictoriaWine." Well, 35 minutes later, I was able to purchase wine and pay the amount of my choice. This is quite worrying because VictoriaWine (http://www.victoriawine.co.uk/) is a well known brand in the UK. What is more worrying is that VictoriaWine doesn't use WorldPay, as previously stated. VictoriaWine uses DataCash (http://www.datacash.com/).

Yes, we had cracked two credit card processing systems within an hour. How many organizations have this problem? How many other systems have this flaw? I attempted to find other customers of these systems without much success. Both companies are discreet about clients. Attempts to discover hyperlinks to the flawed CGI failed. (The search engines AltaVista (http://www.altavista.com/) and InfoSeek (http://infoseek.go.com/) allow searches by URL and by hyperlink, but do not record hyperlinks to CGI scripts or "secure" web pages.) Attempts to search for references were dismal. Most organizations tend to omit the fact that credit card processing is outsourced.

As of May 2000, the VictoriaWine web site (http://www.victoriawine.co.uk/) redirects to a web site that has frames, JavaScript, and MacroMedia Flash. You must enable JavaScript to complete transactions. Purchases may only be made by registered users. This is automated but requires a valid e-mail address and the completion of a survey. Every order requires your e-mail address, so if you don't have one, or you are not willing to supply your e-mail address with your postal address and credit card details, you will be unable to purchase anything.

The demographic survey must be completed before purchases can be made. It is quite lengthy and intrusive and likely to discourage real customers. Fortunately, for our purposes, I have created a test account:

user: billg@microsoft.com
pass: [illegible]

Despite statements on the web site about detection of suspect activity, this account was active and used for private demonstration to various parties over a period of three weeks. Should this account not work, any account can be used to purchase test items. When I first used this system, I placed some items in the shopping basket and then proceeded to credit card payment. From the shopping basket, I accessed a "confirmation" web page that served no apparent purpose and after a pregnant pause I was presented with the form to enter credit card details.

Let's examine that in more detail. I skipped back a few web pages to the shopping basket. I was unable to view the URLs in my web browser because it was a framed web site. To overcome this, I opened the content frame in a new window. Repeating the process I discovered that the credit card form was on the DataCash web site. This would be transparent to the customer during normal use.

With the frame isolated, it was apparent that two intermediate web pages were accessed before credit card details were requested. They both appeared to be blank, one with a VictoriaWine URL, the other with a DataCash URL. I decided to investigate each page in turn. I was dumbfounded to discover that the first web page consisted of a form of hidden fields, including the total price, e-mail address, and a session key, automatically submitting to DataCash with JavaScript. This is appalling practice. Nevertheless, I saved the page, modified the price and accessed it with my web browser.

I was briefly startled before I realized that the web page was scripted to automatically submit the form to DataCash. I was presented with the price of my choice on the DataCash web site. Now we are at the credit card processing stage. When I showed this to staff at Esoteric Hydroponics, they were alarmed that a transaction could proceed so far. Furthermore, what would happen if a stolen or fictitious credit card is used? This was the most prominent concern: is there any verification?

After a long telephone call to WorldPay and finally speaking to a representative of authority, it was discovered that no credit card verification is performed other than checking known stolen numbers. WorldPay collects addresses from customers, but does not currently crosscheck this information. It is not possible to confirm the cardholder's address via WorldPay. Such a system is scheduled for April 2001. The system will be supplied by NatWest. NatWest is also associated with NetBanx, so I assume that the situation would be the same with NetBanx.

We attempted to provide our own verification because third party checking was not of a sufficient standard. We investigated various procedures but were unable to obtain sufficient information from WorldPay.

In general, card processing companies are differentiated by transaction volume. Some companies are suitable for small volumes, others are suitable for larger volumes. Very large volumes are typically done in house. Additional hardware and software required varies widely, as does initial costs. High initial costs may be unsuitable for low volumes, but generally lead to lower ongoing costs. Ongoing costs are typically 2-10% per transaction, although many charge a fixed rate for debit cards. We were unable to find a company that guaranteed payment. For every company encountered, it is the merchant that incurs the cost of fraud. A card number approved by a card processing company may be an unreported stolen card.

Indeed, in any ECommerce dispute between the customer, the credit card company, card processing company, and the merchant, it is the merchant that invariably loses. At present it is possible for any unscrupulous UK credit card holder to purchase goods and then deny knowledge of the purchase. The merchant then receives a "chargeback," which may occur at any time up to 36 months after the purchase. So, an initially profitable enterprise may become unviable if the level of fraud is too high.

Every transaction may be fraudulent. For example, within 24 hours of the Esoteric/WorldPay system going live, a suspect order, slightly less than 2000 pounds, was placed. The order was suspect because unnecessary items were duplicated to obtain the total. The card was approved by WorldPay. WorldPay was contacted by telephone for confirmation. The origin of the card could not be determined but WorldPay recommended that the transaction proceed, presumably due to vested interest of an eight percent commission (160 pounds).

Furthermore, Pukka Seeds was rejected by WorldPay. If you saw a WorldPay application form, you would be very surprised. There is a question asking how an organization would be classified. Staff was unable to find a suitable category. There is a category for pyramid schemes, multiple categories for sex, but nothing suitable for collecting seeds. WorldPay either has a very skewed customer base or knows from direct experience that such companies are lucrative. One would be quite reasonable to assume that the application form was merely a formality for such an overtly tolerant company.

This made the rejection even more of a shock. The whole affair has made my clients disillusioned with ECommerce, despite the fact that each of the two companies has a profitable web site. Staff find it unbelievable that card processing companies provide such a bad service, without risk. The CDROMs sent from Esoteric Hydroponics to potential customers could be tied to the online ECommerce system and credit card payment were it not for a lack of confidence in the system.

By accident, a WorldPay client was encountered during domain name registration. The company is called JustNames, Co. UK (http://www.justnames.co.uk/). The web site uses PHP3 and is so badly written, that it fails to work on NetScape Communicator 4.72 and presumably other web browsers too. During an attempt to register a domain, it was discovered that JustNames Co.UK uses WorldPay and that the price to pay appears in the web page.

It is becoming too easy to fraudulently purchase products online. Many ECommerce web sites are relying on manual procedures to detect problems, if at all. Many organizations are detecting suspect activity, but only because ECommerce orders are scrutinized.

The problem is that most shopping baskets and credit card payment systems are loosely integrated. The credit card payment system is usually on another server and merely receives the total to obtain from the customer. Card processing companies are taking a path of least resistance approach to integration, so as not to dissuade potential clients. In many cases, the integration method is insecure. In some cases, secure methods are employed, while insecure methods remain open. There are many solutions to the problem, none of which have been implemented. Credit card processing companies are taking fat commissions for insufficient service. WorldPay, DataCash, NatWest, and competitors have some explaining to do.

Basic security is being ignored. Numerous web sites have common flaws. Critical data is being passed via client software where it can be tampered with. This information is being trusted by the servers of card processing companies. There are other lapses of security. For example, some companies are not verifying customers sufficiently. This occurs knowingly and action to rectify the situation is tardy. In every case, the merchant pays the price when mistakes occur.

READER DROPPINGS

How Verizon Sucks

Dear 2600:

Think about it. If they can sue you for owning verizonreallysucks.com because they own a mark of "Verizon" then why don't you get a trademark of "Sucks" and sue them for owning verizonsucks.com? Use their own methods against themselves.

Jeff

You'd be astounded how many people have suggested the same thing. But we'd rather win on our terms instead of stooping to their level.

Dear 2600:

I just finished reading the summer issue - great work! I particularly liked the "Over the Verizon" feature on page 16-17. They certainly bought a shitload of names. I myself bought verizonwholesome-speech.com from register.com and using their handy-dandy redirect feature pointed it to 2600.com (hope you don't mind).

Kendall

Even if we did, you have every right to point wherever you want. We cannot let that be taken away.

Dear 2600:

I'd just about finished the letters section of the Summer 1900, I mean 2000, issue, and just for a laugh thought I'd see what was available for the Verizon domain names. I went to Network Solutions to check on verizonsucksass.com, figuring that it'd be taken (it was) but the folks at Network Solutions were nice enough to suggest the following: verizonsucksass.net, verizonsucksass.org, myverizonsucksass.com, everizonsucksass.com, aboutverizonsucksass.com, verizonsucksassonline.com, and verizonsucksasscentral.com.

Oh, and by the way verizonsucksdonkeyass.com is available as well.

Filthgrot

Dear 2600:

I noted with interest when I read the Summer 2000 issue that Verizon has co-opted the peace movement symbol as it is, in fact, trademarked. Yep, that's right. Trademark is held by the Campaign for Nuclear Disarmament in the U.K. (The symbol is made up of the semaphore for N & D.) Of course they don't really pursue it much, well not against ordinary folks. But they have no illusions about the nature of scumbag corporations. Perhaps your lawyers should get in touch.

Salud
Alterego

Dear 2600:

After reading your article on Verizon domains and getting e-mail from gte.net that they were forcing all their users to change their e-mail to verizon.net, I decided to register a few e-mail aliases. I was pleased to find verizon.sucks@gte.net and verizon.sucks@gte.net had not yet been taken. When they get converted, the aliases should be verizonsucks@verizon.net (but I should be using a cable Internet provider by then).

AM

Dear 2600:

I just had another idea for Verizon to deal with. Why don't you file cybersquatting claims against Verizon for VerizonSucks.com. After all, they took the name you planned to use and they aren't using it, are they?

Trouble Maker from WayBack

More Corporate Intimidation

Dear 2600:

You know, ever since these whole CorporateConglomerateSucks.com parody sites got to be such a big deal (thanks to corporate America's lack of a sense of humor), I've begun thinking about the overbearing, buy 'em all out and make 'em part of us, Monopoly Inc. corporation known as Time Warner (or, as I like to call them, Slime Warner). It wasn't until the whole ABC vs. Time Warner dispute that I started thinking about just how much TW owns. Internet: AOL; Television: TBS, CNN, TNT, Turner Classic Movies, Cartoon Network, HBO, Cinemax, the WB Network; Sports: all of Atlanta's sports teams; Stores: Warner Bros. Studios stores; etc. It wouldn't shock me if I were to hear that TW's next move was to buy Microsoft. Where does the greed (and the insanity) end? And these greedy, power hungry, mega corp giants actually wonder why people would want to start up sites claiming they suck? Not to mention the B.S. they claim about copyright and trademark infringement when they're seeking to shut down all "offending sites." Personally, I call all sites of this nature "defending sites." You know, as in defending the right of free speech. When will these parasites learn that until they clean up their acts when it comes to all this crap, they'll always have a hard time making friends with those of us who know about their slimy tactics and greedy, overbearing ways? Keep up the good work at trying to provide something of a wake-up call to these leeches.

7h3 31337 pHr34K4.0id

Thanks, except it's not them we're trying to wake up. As long as individuals get the wake-up call and are willing to stand up to these giants, there is hope. Incidentally, as of right now the Time Warner/ABC deal has not been finalized.

Dear 2600:

We are filing a Class Action suit against Yahoo! and we are trying to rally support. Hope you can help. A federal judge ordered Yahoo! to respond to a request for a preliminary injunction that would prohibit Yahoo! from holding back e-mail messages to coerce credit card data from account holders. Yahoo! e-mail account members who wish to qualify to join the class lawsuit can enroll on-line by completing the questionnaire at www.ExpertsAtLaw.com. This is believed to be the first time the Internet has been used to enroll members of a class action lawsuit.

Yahoo! blocked access to the e-mail account(s) in attempts to obtain personal credit card information before allowing access to e-mail correspondence under the guise of age verification required in the newly enacted Children's Online Privacy Protection Act (COPPA) that became effective earlier this year.

You can also e-mail the head lawyer for more info at: yahooclassaction@aol.com.

LoC

Dear 2600:

I picked up a copy of our local paper yesterday and in a small box on the front page was this headline: "FBI Conducts Raid." My first thought was what the hell is the FBI doing in my suburban Houston neighborhood "conducting a raid?" The house that was raided was only three blocks from where I live and, "according to FBI officials, the raid was part of an ongoing criminal investigation. The warrant was connected to a [yes] Motion Picture Association of America investigation.... FBI officials would not release any information but said a press conference would be held at a later date." What do you think the FBI was looking for there?

dot

Logic would dictate some sort of pirating operation was being investigated. However, the way things have been going lately with the MPAA, it could have had something to do with unauthorized free thought.

Dear 2600:

Apropos your recent entertaining contact with Verizon, I'd like to inform you that some of us out here have simply had it with the state of DNS. Not the actual DNS system which, amazingly, still seems to be functioning fairly well most of the time, but the morass of commercial interests and policy sellouts that makes up the ICANN/NSI system we all have come to know and loathe.

We've set up the OpenDNS project, for which there's a web site at www.opennic.unrated.net. In a nutshell, we're proposing a registrar which will be owned and controlled by the people who have domains registered through it. This registrar will establish top level domains with definite themes and use policies which it will then enforce.

Tobin

Dear 2600:

I'm thinking about registering the domain names 2600sucks.com and 2600arecriminals.com. My question to you: will you fire off formal letters, sic your legal team on me, or generally harass me until I give in? I realize you will probably take offense to the 2600arecriminals.com name but what right do you have restricting my freedoms? If corporations are already threatening people for using "sucks" or "blows" in a domain name, what is to stop them from going after our thoughts next? Will the day come when if I say "fuck NBC" out loud I could face endless legal battles with some faceless entity with millions of times more money and resources than me? In George Orwell's novel *1984*, Big Brother eliminates certain words from the language in order to keep people from thinking unorthodox thoughts. What would you guys do if another company played your game and registered "2600shouldgetsuedbecauseyoursuckstupiddomainnames.com" ?

J-Kast

We're surprised you have to ask. At some point we have to draw the line and fight the intimidation tactics or we'll get to the point where people won't even be able to name their machines however they want, let alone their domains. And it's not as expensive as you might think to register domains, certainly not as costly as giving up your right to free speech.

Dear 2600:

Was just reading the latest edition of *Technology Investor* magazine and noticed their "Website of the Month" was www.chasebanksucks.com. It lists complaints ranging from general screw-overs of their customers to injustices to their employees. There are currently about 400 postings and there have been over 155,000 visitors, so the site has been around a while. I wonder if the owner has received any threatening letters from Chase as you guys have from NBC and Verizon?

Secret Squirrel

Answers

Dear 2600:

I am writing to you regarding Snot Gnome's letter in 15:1 regarding the line graph on his local television service. This channel is used by cable installers to measure the return path signal on the local cable network. The channel is generated by a piece of hardware in the CO's head end that responds to a set frequency sent by the technician's meter. Kind of like a ping reply, if you will. I've used the channel in the past to measure return path signal strength while installing broadband Internet services over the cable network (specifically, @home). If you hook up an oscillator to the cable line and set it to send a signal at the predetermined frequency, you'll see a spike in the line graph on the television set. The higher the spike, the stronger the signal. I haven't discovered much use for this other than troubleshooting network problems while installing @home or other two-way cable devices (i.e., digital cable, digital telephone service). I hope this information helps.

drakkel

IRC Bitching

Dear 2600:

I just wanted to piss and moan about what pricks some of the people are in the IRC hacking channels. Especially some of the operators who just sit in there and kick anybody who doesn't talk about what they want to hear. I'll go in there to try and learn something or ask a question and I'll get kicked because I was asking questions! What a bunch of god damn ass holes. I just saw the Mitnick thing on *60 Minutes* and went and signed on to the mIRC #2600 channel and asked if anyone saw it. Some guy goes "fuck Kevin" and I said how would you like it if you got locked in jail with no trial and then some asshole operator kicked and banned me from the channel. Try it, try going on and asking something and you'll probably be kicked. OK, got that out of my system.

Muckraker

It's IRC. Save your indignation at injustice for real life, where it counts. We guarantee you'll find plenty to bitch about. Incidentally, mIRC is just the program you use and IRC is what you're entering. And each IRC server connects you to a whole different world of channels and people - many of these servers are independent, meaning they're not at all linked. We don't know which server you were using. We recommend the #2600 channel on irc.2600.net but, as always, we exercise no editorial control over an IRC channel. We're sure someone will come along to complain about that.

Dear 2600:

I thought IRC was for chat, 2600 for learning, but I guess I was wrong there. Repeatedly on IRC I have been flamed by people, saying I wasn't "cool" or "1337" because I was using Windows and mIRC (an IRC client that is considered lame by the "elitists" on #2600). My windows computer has DSL, and my FreeBSD and Linux computers don't have ethernet cards or internal DSL modems. I do not want to go out and buy these because I simply do not have enough money and time to configure them. So I choose to use Windows. (All this to explain to you why I don't use Linux or FreeBSD with the Internet, just so you don't think I'm a lamer.) Another thing, I have found it is now trendy to use a type of UNIX over Windows so you can flame those who don't. My friend told me he was sitting in #linux one day and he saw someone coming in. The person had a question because he was new to Linux. The question was "how do I set up PPP outside of Xwindows on Linux?" He was flamed repeatedly and then when my friend tried to tell him the answer, he was kicked and, I found out afterwards, the person with the question was kicked and banned. That made me mad so I asked the person who did it why he did it. So then he came into my channel that I created, #hash-humpers (excuse the name, it's an inside joke), and started yelling at everyone because they were in Windows and using mIRC, and because we, heh, used linkers in Windows instead of compilers in UNIX to do our coding. We later found out he was on a shell account in Windows. These two incidents are not isolated. This has happened to me millions of times after I was searching through my logs. This is what the 2600net IRC server has degraded into, and because of that we've moved to a small, privately owned server. Now we have registered our own domain name and are starting our own IRC server because yours has degraded into a point where everyone, even the real hackers, are snobby people who think they are better than everyone else because they know more.

FLAMEcow

To achieve the kind of atmosphere you want, we would have to monitor and control all dialogue on our IRC server. This just isn't how IRC works. Users define how the conversations go. It makes no more sense to condemn us for unpleasant users than it does to criticize Linux because you got kicked off a #linux channel somewhere.

H2K Videos

Dear 2600:

I was at the web site one day and I was very surprised and happy to see that Jello Biafra would be the keynote speaker at H2K. I don't think there's a better person out there to do it, so good job. Anyway, I'm pissed because I can't go to H2K and I was wondering if there will be any opportunity to maybe buy tapes of Biafra's speech or if there will be a written transcript of it or something like that.

Hedgecore

There should be tapes available soon as well as audio transcripts up on our site as soon as things calm down a little. Keep checking www.h2k.net/post. If you were a speaker at H2K or if you have pictures or anything else to add to the post-convention site, e-mail checkin@2600.com who has been kind enough to volunteer to coordinate all of that.

Questions

Dear 2600:

Why does "^resist" appear in the last bullet on the table of contents in the 17:1 Spring 2000 issue?

Phuct

That's what is known as a printing neglect. It's a hazard of the digital age. Some people see small words and what appear to be significant comments hidden in their issues. Others see Jesus. As always, we apologize for the confusion and inconvenience.

Dear 2600:

There is a problem with my computer. I hope you can help me. Whenever I log on to Internet, often a black window appears like DOS window that says mythis system. Then, after about half a minute, it disappears and my screen flips horizontally.

kamal abbas

The matrix is the Internet. We suggest going outside.

Dear 2600:

Will *Freedom Downtime* be available to non-H2K goers, either online or on VHS tape or DVD, heh?

Thrawn

Yes.

Dear 2600,

I have some work for a good hacker. Would you place an advert in your newsletter? How much? When is copy date? Can you e-mail me sample copy?

Wolf

You win the prize for the largest number of wrong conclusions in a short letter. First, hackers don't go out getting hired simply because they are hackers. We don't take advertising except in our marketplace and that's only for subscribers. We don't charge for this. We don't have "copy dates." And we come out on paper, not via e-mail. A sample copy is $5.

DeCSS/MPAA/DMCA

Dear 2600:

I used to work for one of the "major" Hollywood studios. Let me say this. Illegal distribution of copyrighted material is rampant within these companies. Distribution also occurs between companies of films in media formats different than their current release.

I wish you well on 2600.com's fight against the MPAA. The guidance of this organization is very much blinded. A hard look at the internal policy and procedures of each studio should be conducted before attacking outside sources for providing these materials.

I do not deny that piracy occurs outside of the studios by third parties. However, two of the recent major occurrences of films being available for distribution on the Internet were the result of internal control weakness within the "studio system." The first was a copy of *The World Is Not Enough* becoming available because a film critic released a screening copy. The second was when an Academy screening copy of a particular film (I do not remember the title) in VHS format was available on Ebay. For years now, being able to find an Academy-only screening copy on VHS has been extremely easy. It is because these copies are mailed to Academy members during the Oscar voting period so they can be viewed at home. To easily avoid illegal distribution the Academy should change the policy to force members to visit movie theaters to analyze Oscar nominated films. It is that simple. However, "simple" is not in their vocabulary.

Matt

Dear 2600:

Why is it that the Mac community has not released a Mac version of DeCSS? I am just starting out as a programmer and I simply cannot understand how those who have been programming for many years for the Mac platform have simply laid back and watched while Windows and Linux users are busy coding and porting. Are all the Mac programmers sleeping or am I missing something here? In any case I am wasting no time examining the DeCSS source code, wishing I could understand more.

Anonymous in Iceland

Are you listening, Mac people? This could open up a whole new world of litigation.

Dear 2600:

I've been trying to follow your case but haven't been able to keep up. One thing you might find interesting is that not all DVD's are region coded. I buy a lot of Anime and this stuff is rarely coded for any region. If the disk is going to run in both Japan and the U.S., it makes sense from a business perspective. Anyway, something for you to look into. Thanks for the interesting magazine.

William

A lot of stuff isn't region coded either. But the entire region coding concept is flawed for so many reasons, not the least of which is that it's based solely on greed and on getting people to pay multiple times for the same product. You can expect the same applied to new technologies like HDTV if this is allowed to continue.

Dear 2600:

What's the connection between 2600 and the show *Futurama*? I've noticed at one time a 2600 sign and also "Coming Soon To An Illegal DVD."

beezle

We know that they made reference to the year 2600 once but we never saw a sign. The DVD reference was in the opening title to an episode aired in April. While we don't want to presume that this has anything to do with us, you would be surprised how many people are aware and interested in this case.

Dear 2600:

I have listened to your radio program for years now on the net. I have downloaded the entire archive at this point. The reason I'm writing you today is pretty simple: to give you a good example.

On April 15 of this year my home burned to the ground. With no insurance I was left to pick up the pieces as best I could. I've had the help of many friends and my family. And so far, I've pulled through reasonably well. But, the fire took most of what I owned. Thank god for mp3's! My music collection was hanging in racks with my software on one wall by my computer desk. The racks and jewel cases melted in the heat. Did that mean I was no longer allowed to hear the music I'd paid for the right to listen to? Not a chance. As soon as I could get a computer running again, I began downloading the titles I lost in the fire. I still have a good ways to go but I'm putting a big dent in the task. Nearly 150 albums had to be thrown away as they were nearly transparent from heat damage. I kept as many of the jewel case inserts as I was able to. And as the mpegs are burnt to new discs, the inserts are being matched to the albums. If it weren't for an outlet like Napster, I'd be spending thousands of dollars to replace my music.

Brad Brown

This also brings up an interesting point insofar as licensing. The MPAA and RIAA would like us to believe that we are simply buying a license to view or listen when we buy movies or music. Using that logic, we should still own the license when the physical discs are destroyed.

Dear 2600:

I was reading with interest Jack Valenti's deposition (man, he's an idiot) but I had to wonder what was up with all the confidential stuff? Was it supposedly giving out information on how to tackle the encryption that the Valentites (my word, sorry I didn't want getting out?

But you've got to love the soon to be infamous "Well, one thing they [2600] do is make t-shirts with my picture on it."

phil

While we don't believe Valenti wrote his own material, we do think he's a lot more on the ball than he *appears. For instance, when asked if he knew what Divx was, Valenti said he had never heard of it. Now the questioner was obviously referring to the "new" Divx which is used to compress video signals. But the old Divx was a competing standard for DVDs, one which eventually proved unsuccessful. It is inconceivable that Valenti wouldn't have known about the old Divx if he was at all involved in the motion picture industry. Therefore, when he said he didn't know about Divx, he knew the question wasn't referring to the old Divx and that shows that he had to have known there was a new one.*

Dear 2600:

"'Cable is to the Internet what lightning is to the lightning bug,'" said Jack Valenti, head of the Motion Picture Association of America, at Thursday's hearing." (*San Francisco Examiner*, Friday, June 16, 2000, page B-3).

Now, this kinda shit really pisses me off.

I like lightning bugs. I have a lot of fond memories of lightning bugs. Warm summer nights, trees, green grass, girlfriends. I don't understand what the fuck lightning bugs have to do with lightning. And I really don't understand what all of this has to do with the Internet.

But if Jack Valenti is no friend of lightning bugs then he is no friend of mine.

Decius 6i5

Dear 2600:

At the end of the TV show *Mystery Science Theater 3000*, there was always a short clip called a "stinger" which was a particularly bad part of the movie that was funny all by itself. In a way, it summed up just how ridiculous the preceding movie was.

Following in that tradition, I'd like to submit this as a "stinger" for the recent Valenti DeCSS testimony:

MR. GARBUS: If I wanted to rent *Schindler's List* at Block Buster I could do that?

MR. COOPER: Ambiguous.

Scott

Dear 2600:

I just finished reading your link to Jack Valenti's testimony on DeCSS. What a f#$%ing moron! You'd think he'd at least have been coached a little better from his attorneys. It's amazing such a prominent individual is so willing to make a *total* jackass out of himself. Keep up the great work.

William Ryan

Interestingly, the judge admonished us for questioning Valenti at all, saying it was a waste of time. We think it was very significant in light of the previous comments he had made.

Dear 2600:

After I added my mirror to a few search engines, I was bored and decided to do a search for DeCSS, just to see how many links were broken. The first site I went to was a completely different piece of software called DeCSS. It has to do with Cascading Style Sheets. They have a paragraph declaring their moral support for the *other* DeCSS though. Just thought I should pass the link along. www.gigaling.org/decss.

bappetree

Believe it or not, some of the sites hosting the "fake" DeCSS have gotten threats from the MPAA.

Dear 2600:

I think your stand against the MPAA is one of the most admirable things I've heard of in my lifetime. Clearly, the easier path would be to change your site and forget about the whole thing. But you didn't. Some of the largest and most well-known corporate entities have tried to threaten and intimidate you, and you continue to speak the truth as you know it. Incredibly admirable. Please keep up your good work.

oddOphile

Dear 2600:

On the way home from H2K I had a layover in Baltimore/Washington. I made my way to the bar to consume some overpriced adult beverages and nicotine. As fate would have it, the older gentleman seated next to me with whom I had been conversing turned out to be a Senator from a state where riverboat gambling is really big. I asked if he was familiar with the MPAA suit against 2600 (I was sporting the hat and some shirt by the way). He said that he had heard nothing about it, so I took a few minutes to explain in excruciating detail the entire situation. I even went out of my way to clearly define what a hacker is and voice my disgust at the demonization we as a group have been subjected to by the media as a result of the actions of a malicious minority. It is comforting to know that at least one man on Capitol Hill is now truly informed! Oh God, does this mean I'm a lobbyist now?

QuikFuze
Ward Melville alumni 1984

Funny, this guy had to have voted for the Digital Millennium Copyright Act, which made the MPAA lawsuit possible. It was passed unanimously. It would be nice if every senator could be made aware of the damage their actions have caused. It might just make a difference.

Dear 2600:

Just a quick comment. Does not the law state that everyone has the right to make a copy of their tapes, software, etc. for themselves as a backup? If that is so, and I should be legally able to copy a disk as a backup, a tape, or a CD, then why not a DVD? If that is the case, then I would suggest this be brought up in court. A DVD should be handed to the opposition and they should be asked to make a reproduction for backup purposes as a demonstration to the court that they are not trying to stop people from making legitimate backups in accordance with our laws.

Blanked Out

If only the court was reasonable enough to listen to such arguments. As it happened in our case, the issue of fair use and backup copies was dealt with by suggesting that users get older technology such as videotapes and make whatever copies they need in that way.

Dear 2600:

The idea that there are people in our government trying to criminalize curiosity and intellectual stimulation is beyond frightening. I know this isn't the first time this has happened (Bernie S., Phiber, Kevin, etc.), but it's the first time I've been able to keep informed about it while it's going on, mainly due to your radio show.

One thing I don't have is a lot of time to devote to taking off, picketing, and attending trials. But in place of that, I do have a good deal of money to throw at things. I've donated heavily to EFF with the explicit notice that the funds be tagged for your defense trial. I'm also interested if you have any other organizations representing you that would be encouraged by a donation to take things like this on in the future. I encourage others who are in a similar situation to donate as they can. Also, have you had any direct expenses in this trial, and if so where can I send a check to help with that fund?

Woody

There has been nothing crippling on our end - yet. If that should change, you'll hear about it on our site. For now, please keep the donations coming in to EFF. And thanks for the support!

Misconceptions

Dear 2600:

First off, you guy have a kickass mag. There is no other reading material I look forward to more. There's this older woman who works in my local BookStar who always happens to be there when I go in. The first time she said something like "I wanna be a hacker so I can charge my phone calls to other people." I told her that it was against the law and she gave me the dumbest look I've ever seen. Another time she said she wanted to be a hacker so she could steal credit card numbers. I asked her if she'd ever read a *2600* and kindly explained the difference between curiosity and credit card fraud. Some people just don't have a clue.

pbx

People like this have their ideas conditioned by the mass media. These perceptions are common and they continue to be perpetuated. It can be frustrating but we have to continue to try and educate people so we can avoid the Judge Kaplan syndrome of demonizing entire groups of people and actually applying the law differently to them.

More Info

Dear 2600:

In 17:2, Devil Moon's letter made me realize I should have added the following disclaimer:

"Nobody mentioned in this article was hurt or injured. Please do not under any circumstances attempt to recreate the descriptions contained herein as you and others around you could get hurt, arrested, or even killed. Driving at high speeds is extremely dangerous. Never attempt to turn off your headlights at night while the vehicle is moving. Always wear a seat belt."

For those who do not work firsthand in the auto design industry, you might not know that we often get to drive, tear-down, retool, and rework cars of all models. Engineers often get to modify and add things to cars that normally wouldn't be on them. It's what we do. In fact we have a test track right down the road where we can push cars to their limit. To test their performance above and beyond what they would normally endure day to day. And the test track is where testing should take place, not on the open road.

I did have knowledge of the car. I knew where it had come from, and I knew they had already been driven on the test track. There was a rush to fit new parts on all of them for the auto show, where it was to debut. At the time there were no problems on the car but I knew its X number and could have looked up its name. We mostly refer to cars by an X number. Their commercial names are rarely used.

Another thing he reminded me of is I should have stated that these cars are not built for people to drive like race cars. You should always obey the speed limit and drive according to the appropriate road conditions. Although once you're inside and behind the wheel, a metamorphosis takes over and it's very hard to resist.

The driving at 75 mph really wasn't a big deal. It was from one expressway to another. The speed limit here is 70 mph and there are no points added to your drivers license until you go over 75+ (on I-75 anyway). So 75 really isn't considered much of a big deal, not even by law enforcement. Especially not a big enough deal to label someone a "complete asshole." At 4 am, I-75 is relatively vacant except for truckers. Many a night I have driven for an hour home and seen less than a dozen cars.

The reason I wrote the article was for those who might not be up on today's technology who don't follow the press and publications. I thought people might find it interesting to learn that we are not just working on safety and more gas/energy efficient vehicles (the ones most people think our auto industry is heading to). Even though I will never be able to afford one, I at least understand what is possible and what today's technology is capable of.

SLATAN

Dear 2600:

In 15:4 the letters section mentioned that Mapquest will point out the location of a CO in response to an area code and exchange. There is a more direct way to get this information. Feeding those numbers into the form at www.dslreports.com/coinfo not only returns the address, but every exchange served by the CO, its name, owner, and all the services available from that office.

Will

Dear 2600:

In response to guinsu's article "Securing Web Sites with ASP" in your Spring 2000 issue, I thought I'd provide some additional information that your readers may be interested in.

Under "Making Sure Valid Users Can See Only Their Information," guinsu makes mention of returning the referring page by calling Request.ServerVariables("HTTP_REFERER"). guinsu was right in that you can't fool the browser - but you can fool an ASP page into thinking it has come from a valid URL. The following technique exposes (by making a few assumptions) a potential problem in using only the HTTP_REFERER request.

As an example, let's say we want to fool http://www.hack.org/hack.asp into thinking we were referred by http://microsoft.com/winblows/stackem.htm. First, let's create a localized version of Microsoft.com. Do this by adding (on one line) "127.0.0.1 <spaces> Microsoft.com" to the HOSTS file in \winnt\system32\drivers\etc. Now whenever we type in Microsoft.com in our browser, it will point to our local web server. You could change the value 127.0.0.1 to the IP address of your web server instead. Next we need to create the path \inetpub\wwwroot\winblows\stackem.htm and add it to the list of paths in Internet Service Manager. Add a form to the stackem.htm file pointing it to http://www.hack.org/hack.asp. Now when we type http://microsoft.com/winblows/stackem.htm into our browser, the page appears and our browser thinks it is at microsoft.com! Finally, by clicking a button on the form we are directed to http://www.hack.org/hack.asp having fooled the ASP page into thinking we've come from the correct page.

This may need to be tweaked a little for some installations, but you get the idea. Notice that by using this technique, a valid user of one organization could (at least in theory) gain access to another organization's pages on the same site - assuming permissions were set only at the root level. You may need to clear your cache before experimenting!

Dave/Adelaide
Australia

Dear 2600:

In a followup to the article regarding the SecureID, the easiest way to hack into a system with SecureID protection is to obtain the name of an employee (preferably someone high up) and call into the helpdesk pretending to be that person. Tell them you lost your ID on the plane, etc. and you are trying to login. The helpdesk will always have a spare SecureID connected to the general login ID of one of the staffers there (or the department generally). If your act is convincing, they will give you the ID, pin, and passcode and all you have to do is login. This points out the flaw in any type of remote card accessing system. The card can get lost and a user who needs access will call to obtain another login option.

jeremy

Dear 2600:

I read the article about Taking Advantage of AllAdvantage by silicon bill in the Spring 2000 issue, and I have found how the view bar works. The view bar is mouse and application sensitive only. Meaning that if you stay in a web browser and keep your mouse moving, it will log you as "browsing the web" or you could do what I did. I have a sub woofer, a shoe box, and Goa Trance playing. Tape the box to the top of the woofer, put the mouse inside the box, and turn on your sub woofer. You have to have one that gives a good kick for it must vibrate the mouse to keep it moving! I always have my music on blasting anyway so it doesn't make a difference to me, but if you have roommates or neighbors who don't like loud music that you can hear clearly three blocks away, you should find a different way to keep your mouse moving. I live with a bunch of ravers (much like me) and they like my stuff so it works for me.

Caffeen BoY

Dear 2600:

I have to disagree with Kiss Chin his 17:2 article "More Advantages of AllAdvantage" that you need to surf. It's extremely simple to keep the pages downloading or refreshing in this case. When you refresh, it downloads a new page/image/etc. If you want to use AllAdvantage when you aren't surfing, it's extremely easy. Just go to a site with a webcam. The page refreshes every few seconds so it thinks you are still surfing. Please note that this is untested, as last time my parents had AllAdvantage it trashed their Windows box. Dumb windows bastards.

Mr. Roboto

Dear 2600:

I found a little follow-up info on Bill's write-in about the systems in police cars. I was reading that issue and right after pulled out the "Personal Technology" section of the *Dallas Morning News* and lo and behold there was an article (for the record, I read that section only to laugh and make fun of the editor). The article wasn't about the current tech, but some up and coming stuff. The software is called PacketCluster Patrol and it's made by Cerulean Tech. They say it has secure connections via less so it can't be scanned. The software is installed on Itronix XC6250 Pro laptops with digital packet-based cellular at 19.2kbps. They also say they are planning to expand with Edge and Bluetooth stuff. The Edge tech will allow them 384kbps connections to their cars so they can transmit video in real-time, and they could use Bluetooth to operate small, mobile video cameras when they enter homes or start searching your car because you have a 2600 in the passenger seat. The great part is this: a Mr. Dow with the Ft. Worth police says it's all off-the-shelf stuff so the learning curve is lower. That opens obvious venues for home-testing on how to jam the police transmission equipment. Maybe I'll start reading the Personal Tech section more often.

Bowman

Dear 2600:

A letter in your 17:2 issue from bill brought up an issue with Houston's police department and their use of a laptop in the cruiser. Being another former hacker stuck in the USAF security police duty, I was fortunate (?) enough to learn a little bit about the TLETS system that he referred to.

The TLETS (Texas Law Enforcement Terminal System) is used in most, if not all, police operations in Texas. It's a system that is connected to the NLETS (National Law Enforcement Terminal System) which is connected to the NCIC (National Crime Information Center). The NLETS is run by the collective states and the name may vary state to state, whereas the NCIC is owned and operated by the FBI. Overall, it's a system that allows a patrolman/agent to pull up various "criminal" activities as well as registrations of sorts. Every state, as well as the federal and military agencies, have their version set up differently, but it basically falls under the same principal. It can view (at least on the AFLETS side (Air Force Law Enforcement Terminal System)) at least five different sections: Articles (missing items with recorded serial numbers such as cell phones or camera equipment), License Plates, Vehicles, Persons (wants, warrants, missing persons), and Securities (bonds, bank notes, traveler's checks, and so on). The vehicle/license plate options allow the person to view whether or not the vehicle is registered, stolen, partial registration history, lien holder, addresses, Patent stuff. It's capable of running on laptops in vehicles, but it can run on just about anything. We were running it on an older 386, which I wasn't able to view in depth. As for it being a *nix system, it was graphically stripped, and definitely not Windows, but I believe it ran DOS.

Court Jester

Dear 2600:

In 17:2 Bill wrote about his experience with the computers in police cars and the "see list" network. TLETS is the Texas Law Enforcement Telecommunications Network. It has been around since the 1950's. The Texas Department of Public Safety has a web page on it: www.txdps.state.tx.us/director_staff/information_management/tlets.htm. Until recently it was a 9600 bps store and forward system. Only now is it being converted to a satellite based system to support the bandwidth required for "livescan" applications and other NCIC2000 enhancements. Most states have similar systems. These networks are connected to each other through the NLETS (www.nlets.org).

The Panasonic laptops Bill saw were some version of the Panasonic ToughBook (www.panasonic.com/computer/notebook/index.html) and the Motorolas were MW520 (www.motorola.com/LMPS-RNSG-datamw520/index.html).

WStend

Dear 2600:

In addition to the cars that The Artful Dodger mentioned in response to "Hacking Explorer," the methods should work on any car made by Ford, Lincoln, and Mercury. These are all manufactured by Ford and they use the same components in all of their cars. Ford also owns a number of foreign car companies as well (Volvo, Mazda, Jaguar, Aston Martin, and Land Rover), but as far as I know they only control distribution, not manufacturing, therefore I would imagine it might not work on any of these.

Immolation

Dear 2600:

In response to beatle's article in 17:2 ("Strange Abuses For Your Home Phone"), most of the 1/8 plugs in these types of phones are stereo, not mono like most of the 1/8 plugs we deal with. Although it may work with the purposes he described, it probably won't if you use a mono patch cord and a mono input to your radio (which most are).

lunarul 2085

Dear 2600:

I just finished reading "Java Applet Hacking" in issue 17:2 and wanted to send a little more info about Java jar files. A jar file is actually just a zip file with all of the necessary class files, text, images, etc. that an applet or application need to run packaged up nicely. They use standard zip compression so software such as WinZip (6.0 and up I believe) can open them up. If you unzip it you can use a Java decompiler to get the source code of the applet which should make hunting for passwords easier. Java is apparently easy to decompile unless someone has run an obfuscator on the class files. I have no direct experience with this so I cannot recommend any particular software.

As a side note, you mentioned that the rant on Verizon related domains is really only benefiting the registrars. Well, to reduce that benefit a bit, I suggest two registrars: gandi.net and dotster.com. Both are about $15 a year. The former has very good terms of service (you own the domain name - they are only providing a service).

gainsu

Bypassing Napster

Dear 2600:

For those of you who've been banned by Metallica or Dr. Dre from Napster, I give you the Big Shiny Neat o Swank Workaround.

1. Click on START>RUN and type in regedit.

2. When regedit is open find HKEY_LOCAL_MACHINE\Software\Napster. Click on the napster folder and look on the right side of the screen. Select the key CurrentUser. Press DELETE and click on the plus sign next to Napster on the left side of the screen. Select every folder in the Napster folder one by one. Every time you find CurrentUser, press DELETE.

3. Now press Ctrl + F. When the search window opens type in: 3SD38C13-1434-4B7E-00848304334AA. When it finds a file, delete it. After you delete it, press the F3 key. Delete the next file it finds. Continue until it says "Search Returns No Results" or something along those lines.

4. Now press Ctrl + F again. This time type in: A1A08C13-1381-5348-BXC28E45FF0AAE. Now do the same thing you did in step 3.

5. Now press Ctrl + F again. This time type in: CA05C813-1F34-1B1E-0XC1A4E3FF0AAD. Now do the same thing you did in step 3.

6. Restart your computer.

7. Open Napster. If you deleted all the CurrentUser keys properly it will ask you to set up a new account. Create a new account using a username and e-mail address different than the one you used in your banned account.

8. Napster should be working properly now.

Hedgecore

Mitnick

Dear 2600:

Kevin Mitnick used to make threats and say, "I'm going to kill you, I know who you are and where you live" before he got busted five years ago. If he were really smart he would know cell phones are traceable. How would you feel if a menace hacked into your

2600 web site and changed your index.html file to something you totally disagreed about? And every time you asked or e-mailed the person who hacked you, they just said you suck and you're lame? And if you have to stop what you're doing and fix the web site or hire someone to fix it, that costs money.

This is like if a Lock Master constantly breaks into your house and keeps putting up messages that said your door sucks and your lock is a bubble gum.

The law is the law and if you got busted by what you're doing, then you're not the best.

illii

Every now and then we get anti-Mitnick letters that are somewhat rational but wind up blowing it with some inane or hysterical ranting. You, however, managed to skip the rational part altogether. You also managed not to include any facts at all so we can't even refute them. "Your lock is a bubble gum"?

Dear 2600:

I have been reading your magazine for a couple of years, thanks to my dad who told me to read it one day. I have followed the case of Kevin Mitnick and I even wrote a report about it for my english class. Well anyway, I was looking for skins for the computer game The Sims and found the skin for Kevin Mitnick. Seeing his skin made me smile and I of course downloaded it. You can find the skin at www.simfreaks.com/skinsindex.shtml. I thought you might be interested to know about this.

ReNe12596

Dear 2600:

I know that 2600 is against the fact that Mitnick was held in prison without trial for many years and I agree that it was unconstitutional and I am against what the government did. What I haven't seen is whether 2600 is against the fact that he was charged with computer crimes. I am all for researching how to hack and stuff. Finding ways to do illegal stuff is fun, but I would contact the party responsible for the product with the flaw and instruct them how to fix it, not use that flaw to commit various crimes. What Mitnick did was still against the law and he did deserve to be imprisoned. He was, in my opinion, a criminal. Anyone who commits any sort of crime whether it be on a computer, payphone cheating, or otherwise deserves to be punished. So, what is 2600's opinion on committing crimes over the Internet? I'm tired of "We don't condone hacking for illegal purposes." That is the same as Napster saying "We don't condone the piracy of music." The people in charge of Napster were not really against what was going on. Saying "we don't condone such and such" is just a legal defense. Just to clarify, I am all for Napster and don't believe they did anything wrong. Though I do feel piracy is wrong, those who simply allow other people to do so aren't responsible.

Bill Dahah

Does every "criminal" deserve to be imprisoned? Were the crimes Mitnick was finally charged with anything serious enough to warrant jail time? How come others involved in the exact same activity with Mitnick were never even questioned, let alone punished? It's too simplistic to just label someone as a criminal because they simply broke the rules. It happens all the time. Once you place the criminal label on someone, you can then justify excessive punishment without actually considering the facts. Similarly, if one assumes sensitive information can only be used in bad ways, you can then justify restricting or criminalizing it without realizing the greater danger you're creating.

Reprinting Stuff

Dear 2600:

I work for a medium sized but well known software company and would like to use an article from the latest issue to e-mail to our software testing department. The article in question is: "Finding and Exploiting Bugs" by Astromanob in 17:1. I am a subscriber and I was wondering if I could get the article in electronic form or get the author's e-mail address so I could ask him/her myself. I assure you it would only be used internally and both the author and 2600 would receive credit.

Jason Benton

For the record, and for the benefit of those people (like certain corporations and judges) who can't understand why a hacker magazine has a copyright, we encourage people to send our articles to other people. All we ask is credit for the author and the magazine. You can xerox them, fax them, or whatever. The same goes for material on our web site, our radio show, etc. We speak so people hear what we have to say and it helps us to have our words spread. What our copyright exists for is to prevent people from taking the magazine as a whole and reprinting it as a product. We don't believe in forcing people to buy an issue for every person who reads it, we don't believe in region coding to prevent those in other countries from reading our words, and we don't limit the reading of our words to "authorized" people. Such restrictions have nothing at all to do with copyright. In addition, our writers own their words and they can do whatever they want with them after they appear in these pages. Writers may or may not choose to give out their e-mail addresses - it's completely up to them.

The Old Days

Dear 2600:

I was wondering how your old issues were originally distributed. They were just sheets of paper with holes punched. Did they come stapled together or in a wrapper or something? Just curious about the history of 2600.

Akolade

Originally, 2600 was mailed out as three sheets of paper folded into an envelope with loose leaf holes punched in them. When we expanded to eight pages, we attached the paper so that it was two 11x17 sheets folded to fit in the same size envelope. We'd be interested in seeing recollections from original subscribers on the early days of 2600.

More Government Stupidity

Dear 2600:

According to IDG, people who intentionally spread a computer virus face a seven year prison sentence and a $15,000 fine in Pennsylvania after Governor Tom Ridge signed a new bill into law May 26. The bill also requires that restitution be paid for any damages caused.

The bill, which passed the House and Senate unanimously, makes computer hacking - including denial of service attacks and the willful spread of a computer virus - a crime. It also defines a computer virus for the first time.

This surprised me. Now I don't go writing or releasing viruses at all, but this seems a bit excessive. I'm curious what happens if someone else from, say, Canada released something that affected someone in Pennsylvania. Would they go to Canada to arrest them? It's sad things actually have come to this.

Chad Ziccardi

While releasing viruses or engaging in denial of service attacks are pretty obviously crimes, the hysteria of our lawmakers in dealing with them needs to be reigned in. The punishment has to fit the crime. And we must be especially careful not to encompass nondestructive activities like writing viruses or constructing a denial of service attack into the world of crime. Regardless of how worthless one may consider certain pursuits, the moment writing or inventing becomes synonymous with crime, we've entered into a very scary realm.

Bookstores

Dear 2600:

I was reading in your last issue (17:1) your responses to the Barnes & Noble letters and was struck with the impression that you believe that booksellers don't have the right to choose how publications are sold in their stores. Although I may disagree with a B&N labeling 2600 "indecent" (and I do disagree), I believe it is at the discretion of the company to make that decision. As sad as it may be, we'd be treading on the rights of Barnes & Noble by telling them where to display this magazine. I don't believe Barnes & Noble has the power or authority to limit our freedom of speech in any way. The only true power we have over censorship in this form is to shape the perception of hackers in the eyes of the public so that we're no longer misunderstood or feared.

vesperado

As customers, people have the right to notice and comment when a store isn't living up to their expectations. This is hardly an infringement on Barnes & Noble's rights.

Observations

Dear 2600:

I just got my first 2600 mag ever and my friend tore it up because I spilled juice on his new Playbox. I cried for hours. By the way I love the new Windows 2000. It's super. Lenix and Unix suck with a capitol "X" because they are too hard.

SuperHacker@aol.com

We just can't make this stuff up.

Dear 2600:

I'm glad that you have decided to also put up an mp3 version of your *Off The Hook* files. Not only are the mp3s much smaller in size but they can now be played back on a lot of different applications instead of just Realplayer.

COMFek

Dear 2600:

While playing with my remote last night, I found something quite interesting. On my Time Warner box, if you press 0000 then Exit on the remote while the cable box is off, it switches to a PC mode. I also got it to somehow switch to an AC mode after that. I imagine the PC mode is for cable modems and such as it is equipped with a blocked ethernet jack on the back. Any Road Runner/cable people out there with any idea on what this mode is for and what it does?

wattce

Dear 2600:

With all your payphone articles I thought you might be interested in my experience with US West's 1-800 program and payphones here in Phoenix, Arizona.

A while back I was placing ads in, on, and around payphones. OK, so I have no class. I had competitors whose ads I would remove and if they listed a 1-800 number to respond to, knowing those numbers run $1 or more each call received, I would call that number a minimum of ten times.

I continued this practice for a few months and then one day, after the third call from the same payphone to the same 1-800 number, a recorded male voice would, in a real snotty tone, say, "You have exceeded the number of times this phone may dial a 1-800 number in this 24 hour period." And the call would not connect.

I think I earned that. I caused problems for U S West. I can hardly believe it.

Aulophobe
Phoenix, Arizona

All your sleazy tactics did was activate a block to the number you were calling from on that one particular 800 number. It's not unusual because, unfortunately, neither are people like you.

Dear 2600:

I like how you guys stand up for the "good" hacker community. I think it is wonderful how you try to protect our rights against the corporations which have taken over most parts of our government (funds given to certain politicians by certain corporations). Some people give you negative feedback about what you do but they are just a bunch of scene whores who hang out on IRC all day talking about their drugs and cars. I thank you.

Kevin V.
Trenton, OH

And salaries.

Continued on page 48

FINDING A TARGET USING DNS LOOKUPS

by fU9A5i

So you ve decided you want to hack xyz.com, none of my business why, but you have a problem. How do you find xyz s network in the expanse of the Internet? Firstly, if xyz is connected to the Internet via a dialup link (i.e., ISDN or PSTN - POTS in the U.S.), your job is going to be hard because it s likely that xyz uses a dynamically assigned IP address from their ISP. This IP address is likely to change every time a connection is made from their network to the Internet. They will almost certainly also be using NAT (network address translation) ensuring that their entire network remains hidden behind a single dynamically assigned IP address. Fixed connections (leased lines/private circuits) are however easier to find. This is because xyz is permanently connected to the Internet and the router at their end of the said permanent circuit requires a fully qualified IP address assigned to it. Usually behind this router is some kind of firewall or security device that protects the internal network of xyz from the likes of you and me.

So Where Does DNS Come Into Things?

Most medium (and some small) to large organizations have their own mail servers on site. These mail servers need to be visible from the Internet for that organization to send and receive mail. So to find the xyz network, not just their website which may be hosted at an ISP somewhere, follow the trail of the mail!

When you send mail to auser@xyz.com, a DNS lookup is performed to determine where this mail should be sent. This type of lookup is called a mail exchange or MX lookup; the resulting IP address resolved from this will usually point directly at that company s network. Therefore, mail sent to xyz.com will be sent to TCP port 25 (SMTP) on 195.123.26.2. The IP address is determined from the MX lookup. This IP address may be the company s mail server itself or just the outside interface (network interface) of the corporate firewall. Either way you should have located the network you are seeking.

How To Do DNS Lookups

The hard way is to use the raw nslookup program.

nslookup is the name of a program that lets an Internet server administrator or user enter a host name (for example, microsoft.com) and find out the corresponding Internet address. It will also do reverse name lookup and find the host name for an IP address you specify.

For example, if you entered microsoft.com , you would receive as a response our IP address, which would be something like: 207.46.130.14 or if you entered 207.46.130.14 , it would return microsoft.com .

nslookup sends a domain name query packet to a designated (or defaulted) Domain Name System (DNS) server. Depending on the system you are using, the default may be the local DNS name server at your service provider, some intermediate name server, or the root name server (at InterNIC) for the entire domain name system hierarchy.

You can go directly to the command prompt and type: nslookup microsoft.com , however not all operating systems include this utility (NT and most flavors of Unix do) and if DNS is not correctly configured on your machine it will not work anyway.

The Easy Way

It is far easier to use one of the web-based lookups detailed at the end of this article or to download and use a DNS utility from one of the file mine sites (get one that specifies it can do all types of DNS records).

Here is the dump (from DNScape, http://inetloots.com) of what a complete DNS lookup of the Microsoft domain gives:

```
ATBD.microsoft.com. , microsoft.com , microsoft.com. , NA , NS , 117400 ,
DNS4.CP.MSFT.NET. , microsoft.com , microsoft.com. , NA , NS , 117400 ,
DNS5.CP.MSFT.NET. , microsoft.com , microsoft.com. , NA , NS , 117400 ,
DNS1.microsoft.com. , microsoft.com , microsoft.com. , NA , NS , 117400 ,
dns.CP.MSFT.NET. , microsoft.com , microsoft.com. , NA , SOA , 5915 ,
Resp: msnhst.microsoft.com. Ser:2000071902 Refresh:900 Retry:600
Expire:7200000 Minimum:43200
207.46.130.14 , microsoft.com , microsoft.com. , NA , A , 21914 ,
207.46.130.149 , microsoft.com , microsoft.com. , NA , A , 21914 ,
207.46.130.45 , microsoft.com , microsoft.com. , NA , A , 21914 ,
207.46.131.137 , microsoft.com , microsoft.com. , NA , A , 21914 ,
207.46.131.30 , microsoft.com , microsoft.com. , NA , A , 21914 ,
mail1.microsoft.com. , microsoft.com , microsoft.com. , NA , MX , 26288 , Pref:10
mail2.microsoft.com. , microsoft.com , microsoft.com. , NA , MX , 26288 , Pref:10
mail3.microsoft.com. , microsoft.com , microsoft.com. , NA , MX , 26288 , Pref:10
mail4.microsoft.com. , microsoft.com , microsoft.com. , NA , MX , 26288 , Pref:10
mail5.microsoft.com. , microsoft.com , microsoft.com. , NA , MX , 26288 , Pref:10
ATBD.microsoft.com. , microsoft.com , microsoft.com. , NA , NS , 117400 ,
DNS4.CP.MSFT.NET. , microsoft.com , microsoft.com. , NA , NS , 117400 ,
DNS5.CP.MSFT.NET. , microsoft.com , microsoft.com. , NA , NS , 117400 ,
DNS1.microsoft.com. , microsoft.com , microsoft.com. , NA , NS , 117400 ,
207.46.138.11 , microsoft.com , DNS4.CP.MSFT.NET. , NA , A , 64800 ,
207.46.138.12 , microsoft.com , DNS5.CP.MSFT.NET. , NA , A , 50237 ,
131.107.1.7 , microsoft.com , DNS1.microsoft.com. , NA , A , 20735 ,
131.107.3.125 , microsoft.com , mail1.microsoft.com. , NA , A , 7291 ,
131.107.3.121 , microsoft.com , mail2.microsoft.com. , NA , A , 26288 ,
, , , , , ,
```

So what does all that stuff mean?Basically, what you are looking at is a list of Microsoft s servers with their corresponding IP addresses. In the expanse of the Internet you have just found Microsoft s network. Just look for the MX records....

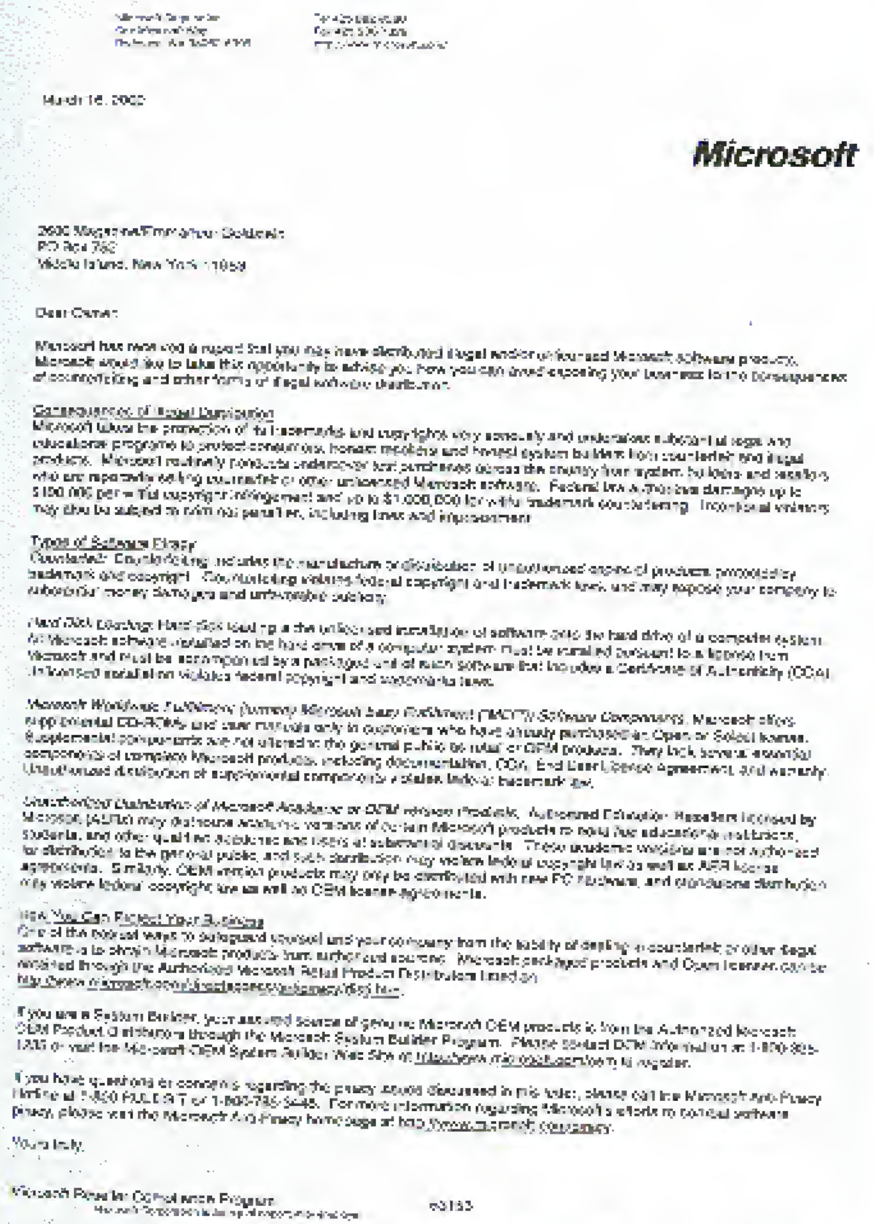
Programs and Web-based Lookups

http://www.simplelogic.com/-Siple/net utils/NsLookup.asp

For Linux system users, here is the Linux manual page for nslookup. http://www.elcafe.com/man/-man1/nslookup.1.html

Trumphurst Ltd. provides a free nslookup program for Windows 9x/NT users.

http://www.trumphurst.com/-dnsocx/nslookup.phtml



Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

Tel 425 882 8080
Fax 425 936 7329
http://www.microsoft.com/

March 16, 2000

Microsoft

2600 Magazine/Emmanuel Goldstein
PO Box 752
Middle Island, New York 11953

Dear Owner:

Microsoft has received a report that you may have distributed illegal and/or unlicensed Microsoft software products. Microsoft would like to take this opportunity to advise you how you can avoid exposing your business to the consequences of counterfeiting and other forms of illegal software distribution.

Consequences of Illegal Distribution
Microsoft takes the protection of its trademarks and copyrights very seriously and undertakes substantial legal and educational programs to protect consumers, honest resellers and honest system builders from counterfeit and illegal products. Microsoft routinely conducts undercover test purchases across the country from system builders and resellers who are reportedly selling counterfeit or other unlicensed Microsoft software. Federal law authorizes damages up to $100,000 per willful copyright infringement and up to $1,000,000 for willful trademark counterfeiting. Intentional violators may also be subject to criminal penalties, including fines and imprisonment.

Types of Software Piracy
Counterfeit: Counterfeiting includes the manufacture or distribution of unauthorized copies of products protected by trademark and copyright. Counterfeiting violates federal copyright and trademark laws, and may expose your company to substantial money damages and unfavorable publicity.

Hard Disk Loading: Hard disk loading is the unlicensed installation of software onto the hard drive of a computer system. All Microsoft software installed on the hard drive of a computer system must be installed pursuant to a license from Microsoft and must be accompanied by a packaged unit of such software that includes a Certificate of Authenticity (COA). Unlicensed installation violates federal copyright and trademark laws.

Microsoft Worldwide Fulfillment (formerly Microsoft Easy Fulfillment ("MEF")) Software Components. Microsoft offers supplemental CD-ROMs and user manuals only to customers who have already purchased an Open or Select license. Supplemental components are not offered to the general public as retail or OEM products. They lack several essential components of complete Microsoft products, including documentation, COA, End User License Agreement, and warranty. Unauthorized distribution of supplemental components violates federal trademark law.

Unauthorized Distribution of Microsoft Academic or OEM version Products. Authorized Education Resellers licensed by Microsoft (AERs) may distribute academic versions of certain Microsoft products to bona fide educational institutions, students, and other qualified academic end users at substantial discounts. These academic versions are not authorized for distribution to the general public, and such distribution may violate federal copyright law as well as AER license agreements. Similarly, OEM version products may only be distributed with new PC hardware, and standalone distribution may violate federal copyright law as well as OEM license agreements.

How You Can Protect Your Business
One of the easiest ways to safeguard yourself and your company from the liability of dealing in counterfeit or other illegal software is to obtain Microsoft products from authorized sources. Microsoft packaged products and Open licenses can be obtained through the Authorized Microsoft Retail Product Distributors listed on http://www.microsoft.com/[illegible].htm.

If you are a System Builder, your assured source of genuine Microsoft OEM products is from the Authorized Microsoft OEM Product Distributors through the Microsoft System Builder Program. Please contact OEM Information at 1-800-365-1235 or visit the Microsoft OEM System Builder Web Site at http://www.microsoft.com/oem to register.

If you have questions or concerns regarding the piracy issues discussed in this letter, please call the Microsoft Anti-Piracy Hotline at 1-800-RULE-BYT or 1-800-785-3448. For more information regarding Microsoft's efforts to combat software piracy, please visit the Microsoft Anti-Piracy home page at http://www.microsoft.com/piracy.

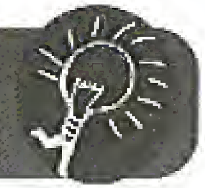
Yours truly,

Microsoft Reseller Compliance Program
Microsoft Corporation is an equal opportunity employer

63153

AIN'T THIS NICE? MICROSOFT DECIDES TO JUST ACCUSE US OF SOFTWARE PIRACY OUT OF THE BLUE. WE HAVE BETTER THINGS TO DO BESIDES USE, MUCH LESS SPREAD, MICROSOFT PRODUCTS. BUT WE'D BE REAL INTERESTED IN SEEING THEIR "EVIDENCE." ON THIS PAGE, WE PRESENT OUR EVIDENCE THAT MICROSOFT ENGAGES IN UNFAIR AND INCREASINGLY BIZARRE BUSINESS PRACTICES. NO WONDER WWW.FUCKMICROSOFT.COM IS SO POPULAR.

Another Way to Defeat URL Filters



by ASM_dood

Cyperpatrol, Websense, SurfWatch, NetNanny - we all know these pieces of software either by reputation or having personally been blocked by one of them while trying to surf the web during work, school, or at home. I'm not certain that it needs to be said that this software often classifies web sites incorrectly or leans heavily towards one end of the political spectrum.

Having laid the groundwork, here is a way to defeat that URL blocker that your parents, school, or corporation have put into place to keep you from browsing what they deem to be "unacceptable."

Take the URL that you are being blocked from going to, such as http://www.2600.com (which is defined as Hacking, Illegal, or Crime depending on the URL filter).

Do an nslookup on the URL and you will get the IP address 207.99.30.230 which is just the dotted octet of its 32 bit number.

Take the individual octet and convert it to its binary equivalent:

207 = 11001111
99 = 01100011
30 = 00011110
230 = 11100110

If any of the numbers are less than eight digits, be sure to pad them out with leading zeroes. Next, string the numbers together:

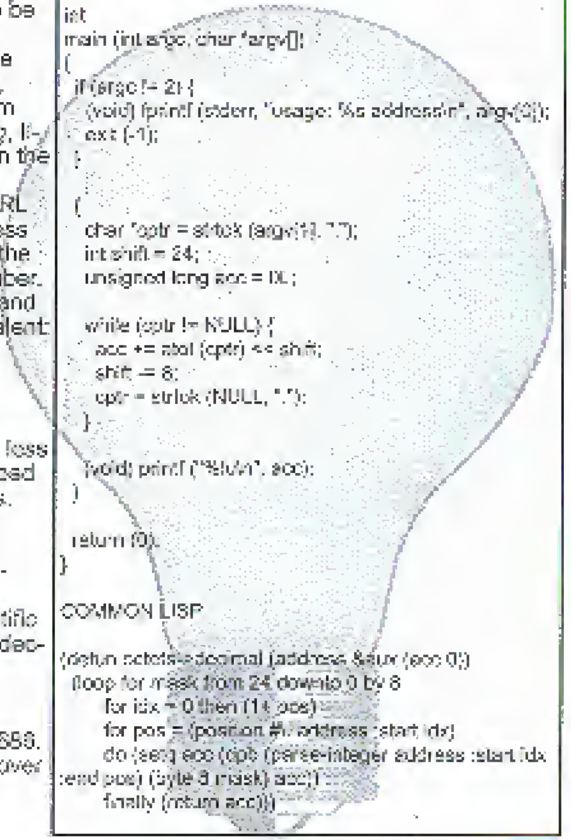
11001111011000110001111011100110

Plug them into your scientific calculator and convert to its decimal equivalent.

In our case:
11001111011000110001111001111011100110 = 3479379686.

So now, we can just surf over to: http://3479379686 and, presto, you are now at www.2600.com.

I'm sure someone else can come up with a script to do the calculations instead of someone having to do them by hand, but I don't have the time or inclination.



A Scrips to do the Calculations
by CSS

C CODE

```
#include <stdio.h>
#include <stdlib.h>
#include <string.h>

int
main (int argc, char *argv[])
{
 if (argc != 2) {
  (void) fprintf (stderr, "usage: %s address\n", argv[0]);
  exit (-1);
 }

 {
  char *cptr = strtok (argv[1], ".");
  int shift = 24;
  unsigned long acc = 0L;

  while (cptr != NULL) {
   acc += atol (cptr) << shift;
   shift -= 8;
   cptr = strtok (NULL, ".");
  }

  (void) printf ("%lu\n", acc);
 }

 return (0);
}
```

COMMON LISP

```
(defun octets->decimal (address &aux (acc 0))
  (loop for mask from 24 downto 0 by 8
        for idx = 0 then (1+ pos)
        for pos = (position #\. address :start idx)
        do (setq acc (dpb (parse-integer address :start idx
:end pos) (byte 8 mask) acc))
        finally (return acc)))
```

Accessing Federal Court Records

by Iconoclast
iconoclast@thepentagon.com

The federal government kindly provides public access to information from almost 200 federal district, bankruptcy, and appellate courts. Documentation such as case and docket information including parties, judges, lawyers, and judgments is readily accessible electronically. This information does not come for free, but it is fairly cheap and affordable for the curious hacker. The system that unifies the access to these records is called PACER: Public Access to Court Electronic Records. The standard PACER service allows access to district court records, while a different system called NIBS (National Integrated Bankruptcy System) allows searches of bankruptcy records including social security numbers! A third system for federal circuit court records is ABBS: Appellate Bulletin Board System.

Access comes in two forms. One is modem dial-up access to each of the individual courts and the other is via the web if it has been implemented for that particular court. There are two dial-ups for each court. One is an 800 number that can be used from anywhere and there is also a local dial-up. For a complete list of both dial-up numbers and all web addresses check: http://pacer.psc.uscourts.gov/cgi-bin/modem.pl. Nearly all dial-ups are set to N81 with VT100 terminal emulation. A few of the dial-ups require pcAnywhere software (passwords listed on the web page) or E71 settings.

The dial-up service costs 60 cents a minute and the web service costs seven cents a page. Billing is quarterly, however it is free to register. A username and password will be mailed to you within two weeks. This username/password combination is a universal login that works across all of the computers in the PACER/NIBS/ABBS systems. You will need to supply your name and address as well as e-mail to obtain an account. The login is in the format of two lower case alpha characters which are the initials of your first and last name followed by four numeric characters. The password is a combination of eight lower case alpha and numeric characters. Check https://pacer.psc.uscourts.gov/regform.html for the online registration form.

Let's say that you've signed up for an account and now you finally get a nice brown envelope in the mail with your login packet. What are you going to do with it? You remember hearing something on the news about Kevin Mitnick being denied a bail hearing and now want to verify the information content and accuracy directly for yourself because you can't believe that such a travesty of justice could occur in this country? Hmm... let's look up Kevin Mitnick's court records! First you warm up your modem and fire up some term software and dial up into the USPCI (United States Party/Case Index) which is a nationwide index of court case information. We will select a criminal search because of the nature of the case and then type in Kevin's name. We find about eight court records. Sometimes the actual records will be stored on the particular court computer where the case was heard. That would require dialing into that specific computer to retrieve the information. Selecting Case Number 2:96cr00881 we then find some astonishing reading. In response to a request concerning the date of a bail hearing we see the dishonorable judge Mariana R. Pfaelzer state: "THE COURT: I AM NOT GOING TO GIVE HIM BAIL." The first federal prisoner denied a bail hearing in United States history! That judge sure knows how to screw up impartial justice.

What about those SSN's on NIBS? After dialing up the court computer and logging in, there is an option "Search by SSN/TAX #", but unfortunately it does not allow wildcards. However, you can instead choose the option to "List New Cases". You specify a date range and you can pull a listing of hundreds of names with addresses and social security numbers of people in your neighborhood, or elsewhere that are having a little financial trouble!

Let's do a brief security analysis of PACER. The restrictions on characters available for password choice make it somewhat weak, however, given the application it may be acceptable. The PACER inquiry computers are on a separate system from the main court host computers which is a very good idea. It means that there will be a delay of about a day in obtaining recently updated court information, but it also prevents Joe Criminal from attempting to erase or modify his court records. The easy availability of massive listings of social security numbers was surprising and could potentially lead to fraud and abuse of a group of people who have already had their share of financial difficulties.

I predict that access to federal court records for the average hacker will become more and more important as our government starts to persecute and prosecute those who engage in honorable technological exploration.

"My people are destroyed from lack of knowledge..." - Hosea 4:6

Zone Scanning

by DEFT
deft@phayze.com

Recently I've been trying to add more focus to my port scanning. By this I mean I try to resist the urge to scan large class B networks that take days or weeks to complete, and which also result in my ISP berating me because they got 10 calls from companies who were annoyed by my massive scans. And all this for what? To know port 139 is open on 800 windows boxes!? Is there a way we can make our scans more efficient and even less noticeable?

What if there was a way to scan only all the "important" machines in a domain (whatever.com)? We would waste less time probing useless machines and probably call less attention to ourselves. By "important," I mean the Web, FTP, NT, UNIX servers, switches, routers, etc., of the company. We would need a way to scan only those addresses and not the other smaller-scale (i.e., users' win95 boxes) machines in between. Keep in mind, all these important machines are spread out over separate subnets. Maybe many of the corporate Web servers sit on the 100.20.4 subnet, and a lot of the more interesting UNIX boxes sit on 100.20.9 and up. That's over 1000 addresses (4*255) in between that we don't really care about since we just want the big players on a company's network. Can this quickly and efficiently be accomplished? Yes! And our answer lies in the DNS system.

DNS is the who's who of the Internet. Arguably any machine that is of significant importance to an organization is registered in DNS somewhere. And this is the information we need. "So how do we get this info Mr. DNS man?" you ask. Well, first of all, I am no DNS specialist. To get more background on this DNS stuff go to www.dns.net/dnsrd/ (lots of great tools too!). Now to answer your question, we will be using something called a zone transfer. A zone transfer is when one machine requests a list of all *registered* machines of another zone. I emphasized "registered" because a zone transfer only obtains the machine names known to the the DNS server you are querying. So if you are looking to probe those other unknown machines (which may be just as important to you as many surprises can be found this way) in between all these major ones, this type of scan is not for you. Note that a zone transfer is a legitimate way for one DNS server to keep its records up to date - there's nothing illegal about it. So it's a great way to get an enormous amount of information from a domain. However, it may look a little odd (read suspicious), and not all domains will allow you to do this.

The programs we will use to do this are host, which runs on Linux (available at www.dns.net/dnsrd/tools.html), and to do the scans, nmap (www.insecure.org), of course. The program host appeared in 2600 a while back. Check out 11:4, "Net Surfing Techniques," page 37 for a quick overview of host. Windows users can participate in zone transfer fun as well. See www.dns.net/dnsrd/mark/wintools.html for some great tools.

The Program

Using a little perl we can make host and nmap achieve our objective of scanning the important machines. Host by itself returns a lot of junk along with the IP addresses. Try running "host -alv whatever.com", and you'll see what I mean. Nmap can't read in these IPs due to this extra junk, so we need to do some cleanup. First, we strip off the DNS junk to get only a list of IPs. (We use IPs instead of hostnames because more than one hostname can be mapped to a single IP (This is virtual addressing. Try "host -alv nbc.com" for an example.) Now although nmap could read this file just fine, there can be many repeating entries of the same IP. So the program then filters out all of these repeating IPs and puts it in a file to be scanned by nmap. So there we are! Now we can scan the machines that matter far faster than a simple bulk scan. This program is made to run on unix but can be easily adapted to perl for NT or even Win98. Try substituting netcat for nmap.

There are two downsides to this method. Firstly, it is loud. Any company with decent security will log a zone transfer. However, this is not to say it would be noticed, as zone transfers are a routine thing. A zone transfer is far less suspicious than your typical TCP-Connect scan, and might even call less attention to itself than a SYN scan, since a lot of IDS's log SYN scans now. In this way, a zone transfer may even be preferred over a scan. When scanning, an IDS would notice thousands of probes, but it would only log one zone transfer. However, the zone transfer is not as thorough. Which brings me to the second downside. Remember, we are only receiving and scanning the hosts registered in DNS. Though we can learn about thousands of machines this way, we could be missing many other important details of the network.

All in all, this method is pretty handy. It is conservative, yet effective. You could also adapt this program to scan only certain types of machines by looking for patterns in the hostnames. For example, many organizations use a naming scheme that gives a hint (if not outright tells you) what the machine is. SUN3.whatever.com, ftp.whatever.com, cisco-5.whatever.com are some examples. Maybe you only want to grab banners from all the ftp servers. You don't even have to use nmap. Be creative!

```
---------------------------------------------------------------
#!/usr/bin/perl

#zonescan.pl - by DEFT

#Usage: zonescan.pl whatever.com


if ($ARGV[0] eq '') {
 die "usage: zonescan.pl whatever.com\n";
}

#do zone x'fer
print "Starting zone transfer...\n";
system("/usr/bin/host -l $ARGV[0] $ARGV[1] > zone");

open(ZONE, './zone');
while (<ZONE>) {
 split;
 if ($_[0] eq "Server" && $_[1] eq "failed:") {
  die "Zone transfer refused.\n";
  }
  else {last;}
}
print "Zone transfer complete.\n";
print "Creating target file.  This may take a while...\n";

#clear old log files for appending to later
system("echo '' > hosts");
system("echo '' > hostsToScan");
system("echo '' > log");

#strip off DNS junk to get the hostnames
while (<ZONE>) {
 split;
 if ( $_[1] eq "has") {
  system("echo $_[3] >> hosts");
 }
}

#need to strip off the repeating entries
open(HOSTS, './hosts');
my(@wholefile) = <HOSTS>;
%seen = ();
foreach $item(@wholefile) {
 push(@uniq, $item) unless $seen{$item}++;
}
for ($i=1; $i<=$#uniq; $i++) {
 system("echo '$uniq[$i]' >> hostsToScan");
}

print "Target file created.  Starting nmap now.\n";
print "Check log for results.\n";

#clean up and do the scan.  Add your own nmap options here.
system("rm -rf hosts zone");
system("/usr/bin/nmap -sS -iL hostsToScan >> log&");

---------------------------------------------------------------
```

Continued from page 5

bomb squad ever showed up and the relaxed attitude of the police made it abundantly clear that there was no threat. The police let the facility reopen ten minutes after the window for the satellite transmission had closed. This was far from an isolated event. In Philadelphia, police repeatedly "inspected" the headquarters of the Independent Media Center during the Republican Convention looking for the most minor of violations in order to shut it down. In addition, helmeted riot cops would surround the building for no particular reason except to intimidate the inhabitants. These exact tactics had been used on Radio B92 in Yugoslavia when they broadcast non-government reports, ironically also using the Internet as their main channel to the world.

On the mainstream networks, none of this was reported. All you saw there were the same boring non-issues. This is what journalism in the United States has been reduced to.

The inspiration of these events along with the tremendous sharing of information and resources that took place at H2K, not to mention all of the crap that's happened to us, has made it clear that we have to work together if we want to have any chance at all of making a difference. That's why we've decided to join with the Independent Media Center to form a base in New York where those who have been shut out and are interested in making a difference can come together, using the net and some imagination to reach the public. You can get more information at www.indymedia.org. No matter where you are in the world, you can participate by opening people's eyes to the issues that have been ignored. Never stop educating yourself on the threats to freedom that keep hitting us day after day. It's about reading, exploring, and communicating.

So now the question remains - what's next for us? It's hard to say. A lot has happened in the past few months. Our documentary *Freedom Downtime* has finally been finished and is now slowly making the hacker convention/film festival circuit. The film, which focuses on the Free Kevin movement and the hacker culture, will be made available on VHS and, yes, DVD in the near future. Our next conference will take place in 2002, a year earlier than normal owing to the great success of H2K and the overall *need* for this kind of thing. Next year we encourage people to attend HAL 2001 in the Netherlands which we believe will be similar in style to a HOPE conference. More details will be published in upcoming issues.

As for how the result of the trial will affect things, we intend to keep doing what we do for as long as that remains possible. We have complied with the injunctions against us but we doubt that will be enough to satisfy the MPAA or future cases that involve the DMCA. At press time, we have removed all links to sites that contain the DeCSS code as per the judge's incredibly misguided ruling. However, we have not removed a listing of those sites. Listing is not the same as linking and if we're ordered to remove a list, then that's one less thing we're allowed to do. We want the restrictions against us to be crystal clear and not open to any misinterpretation.

We don't yet know what the financial ramifications for all of this will be. We encourage people to make sizable donations to the Electronic Frontier Foundation, who have made this fight possible and have expressed the intention to take the appeal all the way to the Supreme Court. Please help make that happen and visit http://www.eff.org/support/joineff.html or send a check/money order to Electronic Frontier Foundation, 1550 Bryant Street, Suite 725, San Francisco CA 94103 USA.

We're not the only victims in this fight - even people who make t-shirts with source code printed on them are being sued now - but if we ultimately lose or if the DMCA is allowed to stand as is, you can bet on an uncountable number of legal battles on the horizon. Support and awareness, for this and all related causes, are the only hope we have for averting this catastrophe.

Continued from page 39

Dear 2600:

I work for a company that is a top 25 company in the Fortune 500. They were trying to merge with Sprint (figure it out yet?). I finished up my training there a couple of months ago and am now working in my hired position. I just wanted to tell you that during our training, they showed us a video, a video about phone phreaking and hacking. It was hosted by the guy that does *America's Most Wanted*. It basically was about a half hour video and it depicted all the phone card schemes and other payphone schemes. During the video, there were a few references to 2600 which were quite amusing. As usual, the hacker was represented as a "bad" guy and dangerous! You guys would probably enjoy watching the video! Let me know if you want it and I'll see what I can do.

Luminol

We've actually had that video for a number of years. But we definitely are interested in any corporate or internal videos of any sort that deal with issues of hackers and computer security. It's always educational to see what kinds of misconceptions are being passed around on the inside.

Dear 2600:

Personally, I consider 2600 a very important and groundbreaking publication. Fifty years from now, 2600 will be compared with *The Crucible*, *The Jungle*, *Uncle Tom's Cabin* and *Common Sense* as literature that was responsible for breaking the foundation of an oppressive corporate body.

To educate these folks, I have found that historic parallels like this have won over many. You just need to know what they know and find a good analogy that they can relate to. You have American history on your side. Eventually, the market or paradigm that they are desperately trying to protect will shift and it all will collapse upon itself. Their own unethical behavior will lead to a lost revenue stream when they find out they are protecting a dead king. Enjoy, you are truly making history.

Stealth Ricochet

That's quite a comparison, one which we certainly don't believe we're worthy of. But thanks for the inspiration.

Dear 2600:

I enjoy your magazine. I also read other computer magazines but find your articles to be the most consistently understandable. The spirit of play, of just plain having fun, is wonderful! Keep up the good work.

Queen Ann

Lotto Fever

Dear 2600:

For anyone actually interested, I just thought this was a little bit amusing. I work at an Xtra Mart in Connecticut, and like many other gas stations, we sell different kinds of Lotto to the many get-rich quick believers. But a few times I have had to reboot the lottery machine responsible for ticket cashing, sales, and generating the "random" numbers for the people's chance to win. The funny thing is that as protective as the CT Lottery wants to be about people trying to cheat the system, this machine is almost an entirely DOS based program handling only the simplest of tasks, basically through different batch files (*.bat). If one was able to plug a keyboard into one of these machines, interrupting and changing how this machine works would be a very simple task.

h0h126

Dear 2600:

I work at a local grocery store in Pennsylvania and I know that all of you are very familiar with the lottery machines and games. It varies from playing a three digit number, four digit number, $100,000 lottery Cash 5, or the big one, the $1,000,000 Super 6 lotto. At least that is how it is in PA. Anyway, after working five hour shifts, you start to get curious and wanna find out how stuff works. Well I did just that in the local mart. See, I was messing around with the keys, pushing two at once or the little gray buttons that are unmarked, and found out some pretty amazing details. Some of the gray buttons, when pushed, bring up another screen. On this screen it shows the login time, name of machine, number of machine (statewide), number dialed, logs, and other cool stuff. (If you are wondering how lottery machines work, they have a 28800 kbps modem in them that connects to wherever the Lotto headquarters are.)

The most interesting thing I found is that if you push that one gray button with the down arrow it gives the login name and password somewhere! You can also find the password somewhere hidden in the store because it is on a little sticker and, at the place where I work, it's hanging so the public can view this. With this password you could cause a whole lot of grief but I would never do such a thing. I am not sure if there is a default password set or anything, but I know you can obtain it by using the machine number (found in the secret menu) and calling the 800 number. I found all this information to be rather funny because they didn't hide it too well. But that is what you get for exploring and knowing a good deal about computers and all. I have learned so much about how the lottery machines work now. I suggest if you work at a place with Lotto machines, find out what hidden menus and options there are! Some may be surprising, others may not. Explore and enjoy!

DigitalZero

The Dangers of Info

Dear 2600:

A while ago, some friends found some security holes and went around cracking sites, reading what precious information they had in them, and defacing the sites. It must have been really fun. But a few months later, I look back at this with remorse. Should they really have done that? They probably cost the company thousands of dollars, got the admin fired, and wasted the time of police investigators. Even though they won't do it again, maybe the information shouldn't have been available to them in the first place. The idea of free information seems more like something hackers are hiding behind rather than a principal. I mean, don't get me wrong, I support freedom of speech, but if we give out information like this it will surely get in the wrong hands. Maybe the government should do things such as not allowing somebody to get on the Internet for a few years if they are caught hacking or not use a phone for several years if they are phreaking. Maybe even shut down sites like hack.co.za because they give away this kind of information. I know that this is goes against a lot of your principals, but can you guys stand idly by when people are having their phone lines rerouted to some payphone in India after getting the information on how to do it from your magazine?

roots11

Look at the progression in your thoughts. You start with remorse over some childish actions and wind up wanting to shut down sites, give the government authority to keep certain people away from computers and even phones, and restrict information because it might get into "the wrong hands." That to us carries more danger than any misuse of information because this kind of control has no boundaries. The most irresponsible use of information is to withhold it out of fear.

Phone Problems

Dear 2600:

I am a new reader to your magazine and although I don't understand some of the tech stuff, I am learning. I thought I could turn to you for advice on my problem. I have AOL as my ISP and they provided me with three local access numbers with which to connect. I confirmed with the operator that these were local numbers for me. Somehow Bell Atlantic made a switch every time I connected to AOL and caused this local number to turn over to a long distance number. My first bill arrived with $875.00 worth of charges to this long distance number which is not even in my computer. I know the first thing you are going to ask me is why do I have AOL. I guess it was the easiest for a beginner like me. No one is willing to help or even pretend to understand this problem. Bell Atlantic throws it to my long distance carrier which is MCI. They in turn blame me and Bell Atlantic. AOL won't help at all saying it's my problem. Reading your magazine made me think you guys would have insight into what I'm dealing with and how to solve it. Maybe you can lead me in the right direction. I'm at my wit's end.

Maria

We've heard of this problem with increasing regularity, especially with online services. We believe it may be related to exchanges owned by competing companies that aren't recognized by the local company. Whatever the problem - and we'd like to hear more theories - Bell Atlantic cannot terminate your service because of a billing dispute with MCI. You should simply tell MCI you never made those calls, period. If you're able to prove that you were connected to a completely different number at the time (call logging, local connection, ISP records), the facts will be on your side.

Dear 2600:

Okay, here's a weird one. I'm sitting at home on line, when my primary phone line rings. Naturally, I check the caller ID and I see:

9:25pm 7/18
123-456-7890
- UNAVAILABLE -

Okay, so I got a spoofed caller ID which I read about a few issues ago. I picked up the line and nobody's there, just a dial tone. The weird part is that my secondary line (which is online) disconnected a few seconds later. Although running out the door and looking over at the NID produced nobody screwing with my lines, I still find this rather weird. Is the telco fucking with my lines? And if they are, do you have any idea what they are doing?

Roark

Although we've never seen this before, it carries the signs of some sort of telco test which first hit your primary line and then your secondary one. These tests aren't supposed to disconnect calls, though. We'd like to know more about this.

Dear 2600:

I'm not a hacker. I can barely boot up and set the margins on Corel 8. I read your magazine to stay informed about the politics of technology. And those letters and their accompanying answers: they're all gems. Now it's my turn. For the last two weeks some wing nut has been calling me at exactly 5:30 every morning. When I answer, there's no one on the line. I called Bell-Atlantic-Verizon regarding annoyance calls. We ruled out an unauthorized wake up service. These were my options: Star 69, Star 57 (a police phone trace), get a new phone number ($40.00), or caller ID with Anonymous Blocker ($7.99 a month). Star 69 and 57 didn't work. I don't feel like shelling out bucks to corporate shareholders just yet. Any suggestions would be much appreciated.

Silverspartan

Note how every solution Verizon came up with involved you giving them money. This is completely unethical. You do not have to pay a penny to stop this from happening. Don't let Verizon tell you otherwise. Contact their Annoyance Call Bureau (the number is in the front of the phone book) and give them the details you gave us. The fact that it happens every day at the same time will make it easy to track. They will contact whoever is doing this and make them stop. However, they won't tell you who's doing it.

Schools

Dear 2600:

I'd like to start off by saying that reading all these horror stories about students being harassed for "hacking" has been making me wonder how people with such a lack of intelligence can make it to positions of power within a school or other organization. I also wonder how it's possible that these incredibly stupid people, who must realize that they know jack shit about computers, feel that it's their right to try and expel or severely punish a student who, with only a few noted exceptions, is only trying to further their education or, as in the case of Code_WarriorX, actually help the system. Anyway, I'm sure that some readers of 2600 must be getting sick of kids writing in with their tales of corrupt systems so here's my story, which may actually uplift the spirits of everyone.

It all started when they upgraded the computer lab at my school last summer to run Linux based PC's, which was nice. Naturally, my immediate desire was to gain root on the system, which I eventually did, and get this: the password was "Finland" without the quotes! How stupid is that? Anyway, I told my best friend the password, and we had a month of fun playing with the computers, non destructively, of course. One day my friend told me that one of the computer staff "knew that we had some type of access to the system," but that she was cool about it. I was a little worried for a while but it passed without issue. Then, later on, the printers stopped working for about two days, and the staff were unable to repair them. So I hacked back into the system and fixed them, allowing lots of students to continue writing their essays and whatnot. The next day, the head computer lab teacher came up to me and said, "I know that it was you who fixed the printers and I don't know how you did it, but thank you." She obviously knew that I must have broken a bunch of the computer lab rules, the punishment for which I could have been banned from the lab or worse, but being a less anal teacher than most, she realized that hacking can actually be used for the powers of "good," and as a result, I went unpunished. In fact, I was never even threatened.

To summarize quickly, the computer lab teacher knew without any doubt for most of the school year that we had hacked into their system and broken every single one of the computer lab rules, but for the sole reason that she was actually liberal and not a tight-ass, superventom stupid-loser-using-power-for-pleasure, she allowed us to experiment with the system and learn a great deal. In fact, had she busted us earlier in the year, the two of us (who had been using Linux for years longer than her) would not have been the little guardian angels we were, fixing things that break when someone badly configures a system. I'm happy that we proved to at least one person that hackers are not to be feared, and that they are capable of true good. I hope that our story serves to remind the hacker community that there is still hope.

Anonymous Hacker in England

It's a two way street. By acting responsibly you were able to reinforce an already positive opinion. It's very easy to create a negative impression by being irresponsible and that will then be used against innocent people in the future.

Dear 2600:

The ID badges have come to town. The county is now spending money keeping track of where we are and what we do by having the badges checked daily by the teachers. Since the badges also have a bar code (with our Social Security number) on them, they are a complete invasion of our privacy as students. If you do not comply with the rules (which we never agreed to or were even told about for that matter), you are given a five dollar bill and progressively harsher punishment.

SwordMage

Dear 2600:

I am a very recent subscriber to your magazine. I just received my first issue today and read the letter sent to you from cs0074life. The part about having to wear ID cards caught my eye. The administrators at my high school in Myrtle Beach, SC also make us wear ID cards that have our picture, name, grade, and (get this) bar code. Yes, we are now bar codes. Sometimes, I question the sanity of our administrators. Unlike P2129 and cs0074life, whose ID numbers resemble those the military use (first letter of their last name and last four digits of their social security numbers), our ID numbers are our social security numbers! And if that weren't enough, the school's database holds the names, addresses, phone numbers, and ID numbers (social security numbers) of every student enrolled in the school. I think that this is a severe security threat to every student in the school.

YorNamHere

Dear 2600:

I am a brand spanking new reader of your lil' 'zine (17:2), and I must say that I am quite impressed. It's nice to get some reminders every now and then that there are some bastions of truly open-minded folks still around. As I was flipping through, I was impressed at the technical sophistication you assume (correctly, I hope) some of your readers possess. But I was even more impressed by the editorial and letters that were printed regarding all kinds of ideas about life, liberty, and general subversion. I was surprised to find a magazine that was portraying ideas that resonated so well with my own few cubic centimeters of brain. An "Editor-In-Chief" named Emmanuel Goldstein who is being sued by the MPAA? That's just too perfect!

Anyway, I'm a young student studying computer science at our fair school of the University of Colorado at Boulder. I have always been fascinated by the way people assume that their philosophy on life is, quite simply, the best, and everyone should be subjected to it regardless of their opinions on the matter. You can see this most clearly in our public educational system, which was brought up over and over in your letters section of this issue. I learned at a very young age that adults are not, in fact, infallible, from this system.

One particular schoolhouse lesson involved my doing some "very bad things" in middle school. We had a "homework hotline" system, where you'd call up, press 1 for homework assignments or press 2 for school events. Well lo and behold, you could press 3, even though it wasn't an option! I pinned this out and found I could record onto any homework box. Being the 13 year old that I was, I proceeded to wipe out half the homework lessons and then brag about it to all of my friends, who proceeded to wipe out the other half. I also used good old trial-and-error to determine a whole mess of other things you could do, like set passwords, create and destroy mailboxes, etc., all of which I did. I'm sure some of you folks are familiar with this type of program.

Predictably, my bragging came back to haunt me. After a few days of teachers unable to take Nirvana's "Rape Me" off of their boxes, they shut the system down and I got called into the principal's office, interrogated for a good two hours, told that "the police were already involved," and generally made to piss my pants. They demanded to know whether or not I had picked the lock of the office that contained the old answering machine computer to do all of this. When I told them I hacked the boxes using my home telephone, they lectured me on how much trouble lying would get me into. I had to pick up the principal's desk phone and show all the eager administrators how they could access all these features for themselves. It's the only time in my life where I've had a principal (or any other schoolteacher) take notes on what I was saying. The best parts ended up being the front page headlines that showed up in our local paper (I lived in a small, inbred, piss ant mountain town, so this was big news), and of course, my brief status as a dangerous member of society. My parents (and all of my friends' parents whom I had gotten involved) were incredibly amused by the whole situation and proceeded to encourage me to screw with the school administration. All of the kids at school thought it was so cool to know a "hacker," even though I knew little about computers back then.

After I educated the educators for a while, they sorta kinda acknowledged that their system (and their knowledge of their system) was a joke, and even thanked me for being willing to fess up about the whole thing. They didn't press any charges and the only punishment I received was to "monitor" the system for a few weeks to make sure someone (me, I think) didn't break into it again. I was surprised at how easy it all was and for years afterwards teachers would want me to set up their e-mail or break a WordPerfect password for them.

I suppose I felt I needed to tell this story because of all the horror stories your readers have sent in. I just wanted to remind you that everyone isn't out to get you. This may seem hard to imagine while you're awaiting the outcome of a major trial or getting screwed by the USSS, but sometimes people can appreciate the humor, sometimes they will acknowledge their own shortcomings, and sometimes they will even let things slide. There is some level of acceptance for "deviants" who want nothing more than to learn, explore, and be amazed at what people are capable of doing.

Herbert

Dear 2600:

I was in the computer lab helping some dumbass AOLers when my computer teacher tapped me on the shoulder. I turned around and he was holding my copy of 2600 and, oh so nicely, kicked me out of the lab because I was "posing a threat." This is so far from the truth. I was sent to the principal, who looked at my confiscated issue and, to my surprise, said, "Did you read that article about Kevin?" We talked for a while about the injustice and I was sent back to class. It relieves me to know that not every school official is a dick.

SSGohan

Someone managed to reach that person and wake him up. We must all try to do the same with others so that one day this won't seem so unusual.

Dear 2600:

I write to you from my desk in ISS (In School Suspension) for not wearing my ID badge. We too have to wear these IDs and if you do not wear them, you have to pay $5.00 and spend a day in ISS. I was sitting here reading cs0074life's letter on the tags, and I also read P2129's letter. And I got an idea - we're going to print flyers for an ID ditch day where we will try to get everyone to leave their IDs at home that day and every day after until they lift the policy. I figure they can't put all 900 of us in ISS. I think it will work - I hope it does.

Tweeter

Fast Food Facts

Dear 2600:

This is to all of you out there who enjoy McDonald's. I work at McDonald's and during my three months of flipping burgers I have uncovered some very interesting information about their computer systems.

The managers at McDonald's have a three digit clock in number. Most managers use their three digit clock-in number as their system access code which is a six digit number. For instance, Sue the imaginary manager has the clock in number of 106. She is not too bright. She uses her clock-in number twice over to make up her six digit password, like 106106. All employees have a three digit number but if you are not management then your number is a double digit represented with a 0 in front like 051.

In each McDonald's, there is a main server in the manager's "office" which controls the entire store. Every order that beeps on the screen is controlled by the system. This system can easily be accessed from a remote location by knowing the number of the store. Here comes the tricky part. It has to ring five times in order for the system to pick up. Easily solved by knowing what time they close. Just call at like three in the morning. (After the store closes people stay around three more hours to clean up.) Once connected you are prompted for a password.

Now we are stuck with the dilemma of not having a manager password. You can get this a couple of ways. First, every Sunday night McDonald's does a system dial-up. This task is completed by the lazy manager before closing. What happens is the manager sends info to the company through dial-up and it prints out a long sheet of receipt paper containing all the hours each employee worked that week and (also) each employee's clock-in number. To obtain this sheet you must do some trashing and get a little messy unless you have connections. The second way to get a manager's number is eat a lot of McDonald's food and wait for an employee to go on break. When the employee orders food they get a half price discount and they need a manager to type in the code so they can get their munchies. Just lean over and flirt with an employee about the same time the unsuspecting manager types in their code.

Big Mac

Credit Files

Dear 2600:

I work in the financial services industry and it strikes me as amazing that so much private information is held by the credit bureaus and financial institutions. Privacy is the responsibility and should be the concern of every individual citizen, but let me tell your readers right now that your consumer credit report contains way more information (correct and incorrect) than you would ever want an anonymous person to know. For the most part there is little that can be done to protect this information from prying eyes. Financial institutions nationwide have ready access to your entire financial, employment, criminal, driving, and spending records without your knowledge or consent. There is some recourse that has been built as a protection against the information being reported incorrectly or falling into the wrong hands, but it does little to preserve your privacy.

As a part of the internal workings of this industry I have more access to your data than you do a lot more. As an example, I can pull a credit report on anyone in the country with little more than their name and a made up address. No social? No problem, when I pull up your info it will politely inform me that the social security number I have entered was incorrect and that the correct one is XXX-XX-XXXX. By the way, when I pull up a credit report I am prohibited by law from giving the customer a copy, and the copy you can request from them (it is your right to get one for free) is not even close to as complete as what I see. Experian, CBI, Trans Union, and Equifax have the goods on you right now. They know where you work, how much you make, how much available credit you have on your cards, who your cell carrier is and how much you use it, whether or not you have been or still are married, where you have applied for credit, and also where and at what rate you spend your money, and a plethora of other tidbits. Credit is extremely necessary for most of us and also extremely valuable but is based largely on arbitrary formulas. This is a system that needs to be hacked and understood. I encourage those of you who are curious, careful, and adept to start snooping (and believe me, there are a lot of back doors). What you find will shock and amaze you.

LOAN RANGER
Colorado

WANT TO HELP?

The best thing you can do to help us as we pursue the appeal of the DeCSS decision is donate generously to the Electronic Freedom Foundation and get as many others to do the same as you can. Every person can make a difference. Send a check or money order to the EFF DVD legal fund at 1550 Bryant Street, Suite 725, San Francisco, CA 94103 USA. You can also donate through the web page at www.eff.org/support/joineff.html.

DeCSS in Words

by CSS

The decryption of data on a DVD encoded through the CSS algorithm can be broken down into three steps. The first is the decryption of the disk key; the second is the decryption of the title key, and the third is the decryption of the encrypted DVD disk sectors.

Each decryption step in software requires the simulation of a 17 bit Linear Feedback Shift Register (LFSR) and a 25 bit LFSR, both of whose outputs are summed eight bits at a time (along with any carry bits from the previous addition) to produce the decrypted output.

There are any number of ways in which the two LFSRs can be simulated in software. The 17 bit LFSR is often implemented using a single machine word where the feedback is computed through cascaded right shifts and XORs. On the other hand, the 25 bit LFSR's output is frequently determined through lookups into byte vectors.

The contents of the low bits in one such lookup table are:
0x00, 0x01, 0x02, 0x03, 0x04, 0x05, 0x06,
0x07, 0x09, 0x08, 0x0b, 0x0a, 0x0d, 0x0c,
0x0f, 0x0e, 0x12, 0x13, 0x10, 0x11, 0x16,
0x17, 0x14, 0x15, 0x1b, 0x1a, 0x19, 0x18,
0x1f, 0x1e, 0x1d, 0x1c, 0x24, 0x25, 0x26,
0x27, 0x20, 0x21, 0x22, 0x23, 0x2d, 0x2c,
0x2f, 0x2e, 0x29, 0x28, 0x2b, 0x2a, 0x36,
0x37, 0x34, 0x35, 0x32, 0x33, 0x30, 0x31,
0x3f, 0x3e, 0x3d, 0x3c, 0x3b, 0x3a, 0x39,
0x38, 0x49, 0x48, 0x4b, 0x4a, 0x4d, 0x4c,
0x4f, 0x4e, 0x40, 0x41, 0x42, 0x43, 0x44,
0x45, 0x46, 0x47, 0x5b, 0x5a, 0x59, 0x58,
0x5f, 0x5e, 0x5d, 0x5c, 0x52, 0x53, 0x50,
0x51, 0x56, 0x57, 0x54, 0x55, 0x6d, 0x6c,
0x6f, 0x6e, 0x69, 0x68, 0x6b, 0x6a, 0x64,
0x65, 0x66, 0x67, 0x60, 0x61, 0x62, 0x63,
0x7f, 0x7e, 0x7d, 0x7c, 0x7b, 0x7a, 0x79,
0x78, 0x76, 0x77, 0x74, 0x75, 0x72, 0x73,
0x70, 0x71, 0x92, 0x93, 0x90, 0x91, 0x96,
0x97, 0x94, 0x95, 0x9b, 0x9a, 0x99, 0x98,
0x9f, 0x9e, 0x9d, 0x9c, 0x80, 0x81, 0x82,
0x83, 0x84, 0x85, 0x86, 0x87, 0x89, 0x88,
0x8b, 0x8a, 0x8d, 0x8c, 0x8f, 0x8e, 0xb6,
0xb7, 0xb4, 0xb5, 0xb2, 0xb3, 0xb0, 0xb1,
0xbf, 0xbe, 0xbd, 0xbc, 0xbb, 0xba, 0xb9,
0xb8, 0xa4, 0xa5, 0xa6, 0xa7, 0xa0, 0xa1,
0xa2, 0xa3, 0xad, 0xac, 0xaf, 0xae, 0xa9,
0xa8, 0xab, 0xaa, 0xdb, 0xda, 0xd9, 0xd8,
0xdf, 0xde, 0xdd, 0xdc, 0xd2, 0xd3, 0xd0,
0xd1, 0xd6, 0xd7, 0xd4, 0xd5, 0xc9, 0xc8,
0xcb, 0xca, 0xcd, 0xcc, 0xcf, 0xce, 0xc0, 0xc1,
0xc2, 0xc3, 0xc4, 0xc5, 0xc6, 0xc7, 0xff, 0xfe,
0xfd, 0xfc, 0xfb, 0xfa, 0xf9, 0xf8, 0xf6, 0xf7,
0xf4, 0xf5, 0xf2, 0xf3, 0xf0, 0xf1, 0xed, 0xec,
0xef, 0xee, 0xe9, 0xe8, 0xeb, 0xea, 0xe4, 0xe5,
0xe6, 0xe7, 0xe0, 0xe1, 0xe2, and 0xe3.

The contents of the high bits lookup table are composed of the following values repeated 32 times:
0x00, 0x24, 0x49, 0x6d, 0x92, 0xb6, 0xdb,
0xff, 0x00, 0x24, 0x49, 0x6d, 0x92, 0xb6,
0xdb, and 0xff.

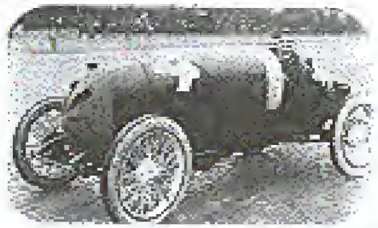
Using this method, one determines the 25 bit LFSR output by using the least significant 16 bits of the LFSR as two eight bit offsets into the above tables, and using the XOR of these values.

The plain text is obtained by summing eight bits of output from both LFSRs plus any carry bits from a previous addition. If an inversion is required, simply XOR the 17 bit LFSR with the inversion mask before summing with the 25 bit LFSR.

Each player is preprogrammed with a small set of player keys. To determine the correct decrypted disk key we must attempt to decrypt the disk key with each of the machine's player keys. The search ends once a decrypted key hashes to the same 40 bit value as the decrypted disk key hash stored on disk. In order to start decrypting keys we must first set up our simulated shift registers. Seed the 17 bit LFSR with the first 16 bits of a player key and set the MSB to 1 to avoid null cycling. Seed the 25 bit LFSR with the next 24 bits (specifically, bits 16 to 39) of the player key. All bits except the three LSBs are shifted up a bit. Bit 4 is set to 1 to avoid null cycling. A table lookup with the LFSR state is used to obtain the next state of the LFSR. A bit inversion of the output is performed with a four state inverter in position 1 for this round of encryption.

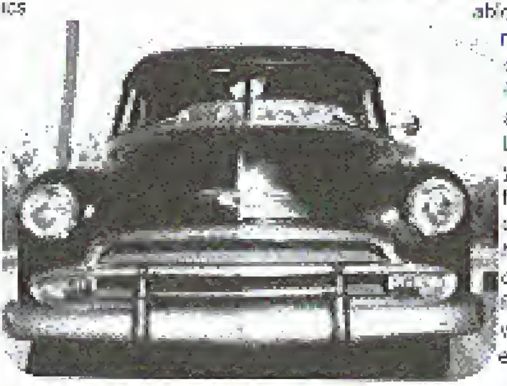
Using the same process that decrypted the disk key, we will now use the disk key to decrypt the title key. The title key is used for the decryption of the encrypted sectors of the DVD disk. The final bit inversion in this round of decryption is performed with the inverter in State 2. Using the title key as input to the shift registers we can now read each sector off the disk and easily decrypt the data blocks using the aforementioned process with the inverter in State 3.

BUILD A CAR COMPUTER



by Megatron

So I'll be driving soon. I realized that I spend so much time by my computer that it would be impossible to go anywhere in my car without at least a bare bone unit in there. So I set out to discover how to create a small unit that would run off the car for super, super cheap. It would be neat to have a computer in your car. You could use it to play MP3's, hack, or as a really complex red box. This article is intended to get you started on the path to an affordable car computer. It's a little more that just sticking a laptop in your car.



As any electronics enthusiast knows there are the two obvious problems: display and power. I hope to cover a few solutions for these as well as info on the unit itself. I'm not a hardware hacker by any means, and some of this is simply speculation (what do you think I'm made of - money?). In research for this article, I saw price tags reach up to 3000 bucks! You could buy another car for that much cash! So let's just take a look and see how far we can stretch our funds.

The Unit Itself

Before we start on the hard stuff, let's cover the actual computer. If you have space to burn, you can use a desktop computer case and just put it by the passenger seat or in the trunk.

If you choose a desktop computer, you pick the specs. If you want lots of ram, fine. I don't really care. The unit I am creating is a 233 mhz, 32 megs of ram crasper I made with spare parts and a decent sound card. If you want MP3 capabilities it's a good idea to have a large hard drive and a good sound card. I'll leave the speaker setup to you. Just go to Radio Shack and buy an RCA to Mini jack to plug into your amp (if you even want MP3's). Just be sure not to put your subs next to your computer if you keep the unit in your trunk. There is already a high risk of hard drive failure with all the vibrations it gets from driving around. If you have a little more cash and want something super small, I suggest looking at the wearable computer community. They have done some amazing things at MIT, and there are Linux boxes that you can carry in a fanny pack. Sound can be an issue here. You have to compromise size for options with wearable computers.

The operating system is up to you. I think Linux would be best - it's not as power hungry as Windows. Plus you can make a cool looking shell for it. Also, it's a good idea to stick in a networking card to transport MP3's and other info.

The Display

In research for this article I read a paper on a "mobile phreak unit." This guy actually put a whole monitor in his car! I don't condone it, but you have to work with what you have. The best idea is a small LCD screen that is simple to install. We want to keep it as basic as possible - don't want anyone to electrocute themselves.

The best place to get LCD screens cheap is electronic surplus stores. I really liked http://www.allelec.com/VGALCD.html kits. This is by far the best solution for our needs. 89 bucks for an ISA card that works with most every OS and a 640x480 capable 5 7/8 x 10 3/8 9.6 in monochrome display. Just plug the card into the motherboard and you're good to go. The only problem is that card is ISA, not PCI. This is okay for most people, but if you are starting from scratch and want this display type, be sure to buy a motherboard with at least one ISA slot. This is not a good display choice for DVDs. That good a screen will cost about 200 smackers, but still cheaper that any commercial unit.

If you are a good EE you can design a super small MP3 player that will fit either under your seat or in the radio compartment of your car with a small LED display.

The Power

Like I said before, I am no hardware hacker and when it comes to power, I know squat. I turned to the Internet for help and guidance in these desperate times. I am using a Statpower PortaWattz 300 DC to AC power inverter in the unit I'm making. I got this idea from Riskable's car computer (see below). He plugs it into the cigarette lighter instead of the battery because if his computer crashes he can reboot it. He also grounded the power by means of a ground loop isolator so he didn't get any hum. Go to his site for more info. If you smoke and want to keep the unit in the trunk, I think a switch would work fine.

The Interface

This one is simple. A keyboard and mouse are the cheapest ways to go. If you go this route, I suggest getting a cheap wireless keyboard and a wireless or touch pad mouse. You could try to find a mini keyboard or modify a laptop keyboard. This is entirely up to you. Be sure to have long wires if you keep the unit in the trunk.

Conclusion

If you have an old computer and a few hundred bucks to spare, I suggest making a car computer. Let's give it a name: The Econoline Carcomp 8000. Yeah, that's cool. Now let's get ready for some Hard-Driving!

Components

A 233 mhz computer with 32 megs of ram, 10 gig HD case: free (spare parts)
A StatPower Portawattz 300 watt
Power Inverter: $50
A 640x480 capable 5 7/8 x 10 3/8 9.6 in monochrome display with controller card: $89
A Ground loop isolator: $10
Touch pad mouse: $20
Total: $169
It cost me 169 bucks to
adapt a computer to a car.

Resources

Computer itself

http://riskable.youknowwhat.com/car.html - Some guy called Riskable who made a car comp without a screen. Always an option.

http://rehmi.www.media.mit.edu/people/rehmi/HackMan0.4.html - Hackman wearable computer.

http://wearables.www.media.mit.edu/projects/wearables/ - MIT wearable computers. *Really* neat stuff.

http://dir.yahoo.com/Computers_and_Internet/Mobile_Computing/Wearable_Computers/ - wearable computer links at Yahoo.

Display

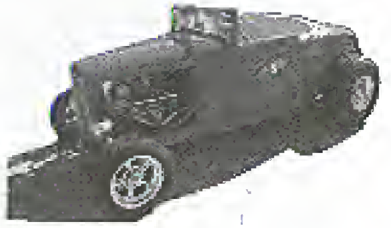
http://www.allelec.com/VGALCD.html -Best display options.

http://www.elo.com - A great source for all sorts of surplus electronics.

http://www.igadget.com/igadget/cartelevisions.html - Go here to see what the mainstream prices are (very *high!*).

Power

http://globe-mart.com/electron/power/inverters/statpower/PW300.htm -
Got the inverter for 50 bucks.



Marketplace

Happenings

PHREAKNIC is Nashville's fifth annual hacker con. It will be a weekend of hacking, panel discussions, partying and other mayhem at the Days Inn - Airport/Opryland area, 1 International Plaza, Nashville, TN 37217-2011, November 3-5, 2000. More info at http://www.phreaknic.org.

CHAOS COMMUNICATIONS CONGRESS 2000 will take place December 27-29 at Haus am Kollnischen Park in Berlin, Germany. Feel free to mail any suggestions for workshops, lectures, speakers, or other things to congress@ccc.de. More details will be posted at www.ccc.de/events/congress2000/.

HAL 2001 (Hackers At Large) is an event scheduled to take place on August 10, 11, and 12, 2001 in Enschede, the Netherlands. HAL 2001 will be a three day, open air networking event in the tradition of HEU '93, HIP '97, and CCC '99. The event will focus on computer security, privacy, citizen rights, biotechnology, and other controversial issues affecting society as a whole. For more information or to get involved in the organization, visit http://www.hal2001.org

For Sale

CYBERCRIME DIGEST. New publication focuses on issues of the millennium including privacy, Internet fraud, security, and cyber legislation. This is a nontechnical, non-glossy publication geared toward the average computer user. We hope to include editorial content from the "hacker's perspective" to make our readers aware of varying philosophies concerning the topics on hand. Subscription rate is $20 per year for six issues. 2600 readers can obtain an introductory copy by mailing a check or money order for $3 to CyberCrime Digest, 5027 N. Socrum Loop Rd #109, Lakeland, FL 33809.

HACKERS WORLD, 660 MB of hacking files $15. Anarchy Cookbook 2000 $25, Virus 2000 (351 pages of computer viruses) $10, Make Money Fast (250 ways to make money on the Internet) $5, Phone Ring (no plans, the real device) $10, cell phone pickup device (just dial at the phone and hit the button and it picks up the call with fake static) $20 for plans and $30 for the device. Send all orders to: 700 Fairl Dr. A107, Glendale, CA 91207. Make all checks out to Sugar

HTTP://WWW.PAOLOS.COM, since 1996. We offer lockpicking and auto entry tools, confidential book publications, Crimean adult air rifles, and an exciting line of switchblades, FFL transfers in PA: pistols, shotguns, rifles. We guarantee what we sell UNCONDITIONALLY for 30 days. In addition to factory warranties, and will beat the competition's prices on anything! No "spy store" hype here. We ship internationally, and will only sell to qualified customers. Now accepting Visa/MC from US. customers.

COMPLETE TEL BACK ISSUE SET (devoted entirely to phone phreaking) $10 ppd. CD-ROM PDF/ASCII version with lots of extra data and plans for voice changers, scramblers, tone boxes, bugging, etc. $14 ppd. Forbidden Subjects CD-ROM (330 mb of hacking files) $12 ppd. TAP back issue set (full sized copies) $40 ppd. Pete Haas, PO Box 702, Kent, OH 44240-0013.

THE E-HOLSTER is a durable, high technology product that is basically a shoulder holster that enables you to comfortably carry from two to four personal appliances/items inside of very flexible, yet protective black neoprene or black leather pouches with safety straps. For complete information and purchase, go to http://www.eholster.com

CRYPTO OUTLAW T-SHIRTS. Governments around the world are turning innocent people into crypto outlaws. Where will the madness end? Cryptography may be our last hope for privacy. From Cursedspace, the unofficial band of anarcho-capitalism. Get yours at cursedspace.org/t-outlawcrypto.html.

PLAY MP3S IN YOUR CAR OR HOME: Mp3 juke unit plays mp3 cd, cdr, and cdrw discs. Can be mounted in car, home, or even inside a free drive bay of a PC. It can be trunk mounted in a car or placed under the dash. The unit is self contained, pre-assembled, and it includes a wireless remote. For more information, visit http://www.mp3carplayer.com/2600 or e-mail 2600@mp3carplayer.com. Sign up for our affiliate program and earn some cash. Resellers needed. $25 from every 2600 sale will go to the Kevin Mitnick fund. We will ship anywhere that we can.

REAL WORLD HACKING: Interested in rooftops, steam tunnels, abandoned buildings, subway tunnels, and more? For a copy of Infiltration, the zine about going places you're not supposed to go, send $2 to PO Box 66025, Town Centre PO, Pickering, ONT L1V 6P7, Canada.

HACK THE RADIO: Hobby Broadcasting magazine covers DIY broadcasting of all types: AM, FM, shortwave, TV, and the Internet. It includes how-to articles about equipment, station operation and programming, enforcement, and much more. For a sample, send $3 U.S. ($4 Canada or $5 international). A subscription (4 quarterly issues) is $12 in the U.S. Hobby Broadcasting, PO Box 642, Mont Alto, PA 17237.

INFORMATION IS POWER! After years of being in the scene we've put together a publicly accessible site for people to talk about a wide variety of hacking games. In addition, we have obtained feeds for our own private news center for information and articles about current computing happenings worldwide. You can find all this, and more, on our site at: www.subnetz.org/gorm.

THE BEST HACKERS INFORMATION ARCHIVE on CD-ROM has just been updated and expanded! The Hackers encyclopedia '99 - 12,271 files, 650 megabytes of information, programs, standards, viruses, sounds, pictures, lots of NEW 1998 and 1999 information. A hacker's dream! Find out how, why, where, and who hackers do it to and how they get away with it! Includes complete YIPL/TAP back issues 1-91! Easy HTML interface and DOS browser. US $15 including postage worldwide. Whirlwind Software, Unit 606, 103 911 Yates St., Victoria, BC Canada V8V 4Y8. Get yours!

Help Wanted

CREDIT REPORT HELP and checksystems. Absolute confidentiality. stinews@excite.com.

HELP WITH CREDIT REPAIR. All 3 credit reporting agencies. R.A., PO Box 1611, Julian, CA 92036-1611 or rar1036@yahoo.com.

NEED HELP WITH CREDIT REPORT. Lucrative reimbursement for services. Help clean up mess. Please reply PO Box 5189, Mansfield, OH 44901. fax 419-756-3066 or phone 419-756-5644.

LOOKING FOR ASSISTANCE in matching names and addresses to known telephone numbers. Existing "reverse" search programs have not been helpful. Willing to pay reasonable fee for each match. Call (718) 261-0565 for further details.

POLITICAL PRISONER has non-profit organization, developed his own print or web pages to foster defined support for his release, but has no one to post his work on the Internet. Needs someone to post it, maintain web pages (updating), and maybe improve the cosmetics. Has money to pay for the site (www.SwanEmergency.org). Also need mailing lists at reasonable costs. Anyone interested may contact: Barb LeMay, Director, Sean Swan Emergency Campaign, P.O. Box 57412, Des Moines, Iowa 50317. (515) 265-2306

NEED HELP ON CREDIT REPORT, ex wife screwed me. Please reply to: HNR, 5201 W FM. 1960, PMB#215, Houston, TX 77069. "Michael"

I AM INTERESTED IN HIRING SOMEONE familiar with accessing telephone information. Generous pay. Please contact me at C. Chau, PO Box 276, Middle Village, NY 11375.

NEED HELP WITH CREDIT REPORT. Please respond to B. Mendel, 433 Kingston Ave., P.O. Box 69, Brooklyn, NY 11225.

HELP TO FIND TROJAN HORSE PROGRAM. Understand there is a Trojan Horse program which may be added as an attachment to an email (which appears innocuous when viewed or read) but which will execute and record any password used by the recipient and then send it by e-mail to an outside recipient. Further, that if the outside recipient doesn't receive it for any reason, the e-mail message with password(s) will not bounce back to the sender. Also, there is another Trojan Horse program which, after it installs itself in the UNIX based ISP of the target, will mail out copies of all incoming/outgoing to an outside recipient without the target being aware of it. Can anyone help with complete information, details, and programs? bryn05@usa.net

Wanted

LEGAL PROFESSIONAL(S) and/or law students from BRAZIL and ARGENTINA to help pursue various issues of wrongdoing committed by members of the Brazilian Bar and possibly the Argentine Bar. All claims of unethical conduct, failing to act competently, and obstruction of justice are substantiated by documented facts. I am an American citizen, wrongfully treated by well-paid Rio de Janeiro, Brazilian lawyers CARLOS ROBERTO SCHLESINGER and NELIO ROBERTO SEIDL MACHADO. Because of their incompetence and malicious disregard for established law(s), I find myself incarcerated in an American prison with little hope of finding freedom unless I am able to obtain help from an intelligent, resourceful, and dedicated lawyer, law school professor, and/or law student(s). The above-mentioned claims are easily verifiable through existing records. Many have been posted within my web site, and the person(s) interested in lending me a much needed hand will help expose some of the rampant corruption that is to be found in the Brazilian and American legal systems. Only by contacting the Lawyers Professional Conduct Committee of the State of Rio de Janeiro, Brazil, and requesting to have Attorney SCHLESINGER and MACHADO stripped of their law licenses, will foreigners and Brazilians alike be afforded justice in Brazil. For additional information and review of court documents, go to: www.brazilboycott.org.

MINIATURE PEN MICROPHONE that is very sensitive and transmits at least 300 feet to an FM radio. Need the name/address of manufacturer(s) (and prices if available). Reply to bsitz@juno.net

I'M LOOKING FOR THE ORIGINAL/OFFICIAL TAP MAGAZINE/NEWSLETTER. Contact me if you have any information regarding the original TAP phreaking magazine/newsletter. I suggest you provide the condition of the magazine/newsletter and the price that you would want for it when e-mailing me at mrmrock36@hotmail.com or icq 13033226. I want the ORIGINAL copies only.

WANTED: Heathkit ID-4001 digital weather computer in working condition. Also wanted, microprocessors for Heathkit ID-4001, ID-1890, ID-1990, and ID-2090. Advise what you have, price, and condition. E-mail: heath.39@usa.net

Services

CHARGED WITH A COMPUTER CRIME in any state or federal court? Contact Dorsey Morrow, Attorney at Law and Certified Information System Security Professional, at (334) 265-6002 or visit at www.dmorrow.com. Extensive computer and legal background. Initial phone conference free.

SUSPECTED OR ACCUSED OF A CYBERCRIME IN THE SAN FRANCISCO BAY AREA? You need a criminal lawyer committed to the liberation of information who specializes in hacker, cracker, and phreak defense. Contact Omar Figueroa, Esq., at (800) 935-6061 or (415) 986-5591, at omar@alumni.stanford.org, or at Pier 5 North, The Embarcadero, San Francisco, CA 94111-2030. Free personal consultation for 2600 readers. All consultations are strictly confidential and protected by the attorney-client privilege.

Announcements

FREEDOM DOWNTIME is the new feature-length 2600 documentary playing at hacker conferences and film festivals. Keep checking www.freedomdowntime.com for possible showings in your area as well as details on VHS and DVD availability.

MOVE MONEY ANONYMOUSLY or anonymously as you see fit. Galaxy's only hacker-operated transaction service http://www.tipper.com/occupy/Galaxy.html. Collect donations from any web page.

OFF THE HOOK is the weekly one hour hacker radio show presented Tuesday nights at 8:00 pm ET on WBAI 99.5 FM in New York City. You can also tune in over the net at www.2600.com/offthehook or on shortwave in North and South America at 7415 khz. Archives of all shows dating back to 1988 can be found at the 2600 site. Your feedback is welcome at oth@2600.com.

Personal

IMPRISONED HACKER welcomes communication from the outside world. Zyklon, accused of hacking the White House web page, can be reached at zyklon@2600.com or directly through the mail: Eric Burns, #43726-065, Unit 5 (ED7-1810), PO Box 6000, Sheridan, OR 97378-6000.

I AM A FAIRLY INTELLIGENT PERSON with potential to be a computer geek looking for someone to give me one-on-one lessons in areas necessary to be a hacker by way of correspondence. I am presently being held captive by the Texas prison system and I have approximately 2 years before I am released and I want to familiarize myself with the basics and fundamentals of hacking during this period. Interested people contact me at: T. EDWARD JONES, No. 510071, HC 67, Box 115, Kenedy, Texas 78119, U.S.A.

ONLY SUBSCRIBERS CAN ADVERTISE IN 2600! Don't even bother trying to take out an ad unless you subscribe! All ads are free and there is no amount of money we will accept for a non-subscriber ad. We hope that's clear. Of course, we reserve the right to pass judgement on your ad and not print it if it's amazingly stupid or has nothing at all to do with the hacker world. All submissions are for ONE ISSUE ONLY! If you want to run your ad more than once you must resubmit it each time. Include your address label or a photocopy so we know you're a subscriber. Send your ad to 2600 Marketplace, PO Box 99, Middle Island, NY 11953. Include your address label or photocopy. Deadline for Winter issue: 11/15/00.

ARGENTINA

Buenos Aires: In the bar at San José 05.

AUSTRALIA

Adelaide: [illegible] Snack Bar on the corner of Grenfell & Pitt [illegible] Streets. 6 pm.

Brisbane: Hungry Jacks on the Queen St. Mall (RHS, opposite Info Booth). 7 pm.

Canberra: KC's Virtual Reality Cafe, 11 East RW, Civic. 6 pm.

Melbourne: Melbourne Central Shopping Centre at the Swanston Street entrance near the public phones.

Perth: The [illegible] in [illegible] Murray Street (near [illegible] William Streets). 6 pm.

Sydney: The Crystal Palace, front bar/bistro, opposite the bus station area on George Street at Central Station. 6 pm.

AUSTRIA

Graz: Cafe Haltestelle on Jakominiplatz.

BRAZIL

Belo Horizonte: Pelego's Bar at Assufeng, near the payphone. 6 pm.

Rio de Janeiro: Rio Sul Shopping Center, Fun Club night club.

CANADA

Alberta

Calgary: Eau Claire Market food court (near the "wall of fire").

Edmonton: Sidetrack Cafe, 10333 112 Street. 6 pm.

British Columbia

Vancouver: Pacific Centre Food Fair, one level down from street level by payphones. 4 pm to 9 pm.

Quebec

Montreal: Bell Amphitheatre, 1000 Gauchetière Street.

ENGLAND

Bristol: Next to the orange and grey payphones opposite the "Galleries" mall, Merchant Street, Broadmead. Payphones: +44 117 9299011, 9294437. 7:30 pm.

Hull: In the Old Grey Mare pub, opposite The University of Hull. 7 pm.

Leeds: Leeds City train station outside John Menzies. 6 pm.

London: Trocadero Shopping Center (near Piccadilly Circus), lowest level. 7 pm.

Manchester: Cyberia Internet Cafe on Oxford Rd. next to St. Peters Square. 7 pm.

FRANCE

Paris: Place d'Italie, in front of the Grand Ecran Cinema. 6:30 pm.

GERMANY

Karlsruhe: "Old Dublin" Irish Pub, Kapellenstrasse, near public phone. 7 pm.

GREECE

Athens: Outside the bookstore Papasotiriou on the corner of Patission and Stournari. 7 pm.

INDIA

New Delhi: Priya Cinema Complex, near the [illegible] Showroom.

ITALY

Milan: Piazza Loreto in front of McDonalds.

JAPAN

Tokyo: Ark Hills Plaza (in front of [illegible]) [illegible]. 6 pm.

MEXICO

Mexico City: Zocalo Subway Station (Line 2 of the "Metro", blue line). At the "Departamento del Distrito Federal" exit, near the payphones & the candy shop, at the beginning of the "Zocalo-Pino Suarez" tunnel.

POLAND

Stargard Szczecinski: Art Cafe, Bolesława [illegible]. 7 pm.

RUSSIA

Moscow: [illegible] Tower cafe near [illegible] (Telephone Agency of Moscow/Telegraph Agency of Soviet Union) - [illegible] Arbat.

SCOTLAND

Aberdeen: the Bowling Station.

Glasgow: Central Station, payphones next to Platform 1. 7 pm.

SOUTH AFRICA

Cape Town: At the "[illegible]" food court.

Johannesburg: Sandton food court.

UNITED STATES

Alabama

Auburn: The student lounge upstairs in the Foy Union Building. 7 pm.

Birmingham: Hoover Galleria food court by the payphones next to Sbarro's. 7 pm.

Tuscaloosa: University of Alabama Ferguson Center by the payphones.

Arizona

Phoenix: Peter Piper Pizza at Metro Center.

Tucson: Barnes & Noble, 5130 E Broadway.

Arkansas

Jonesboro: Indian Mall food court by the big windows.

California

Los Angeles: Union Station, corner of Macy & Alameda. Inside main entrance by bank of phones. Payphones: (213) 972-9519, 9520; 625-9923, 9924.

Sacramento: Round Table Pizza, 127 K Street.

San Diego: Leucadia Pizzeria on Regents Road (Vons Shopping Mall).

San Francisco: 4 Embarcadero Plaza (inside). Payphones: (415) 398-9803, 9804, 9805, 9806.

San Jose: Orchard Valley Coffee Shop/Net Cafe (Campbell).

Connecticut

Bridgeport: [illegible] Pizza, [illegible] Mall [illegible].

District of Columbia

Arlington: Pentagon City Mall in the food court.

Florida

Ft. Lauderdale: Broward Mall in the food court by the payphones.

Ft. Myers: At the cafe in Barnes & Noble.

Miami: Dadeland Mall on the raised seating section in the food court.

Orlando: Fashion Square Mall in the food court between Hovan Gourmet & Panda Express. Payphones: (407) 895-5238, 7373, 4648; 896-9708; 895-6044, 6055.

Pensacola: Cordova Mall, food court, tables near [illegible]. 6:30 pm.

Georgia

Atlanta: Lenox Mall food court.

Hawaii

Honolulu: [illegible] Coffee Shop, [illegible]. Payphones: (808) [illegible], 808-528-5252.

Idaho

Pocatello: College Market, 604 South 8th Street.

Illinois

Chicago: Screenz, 2717 North Clark St.

Indiana

Evansville: Washington Square Mall food court.

Ft. Wayne: Glenbrook Mall food court. 6 pm.

Indianapolis: Circle Centre Mall in the StarPort/Ben & Jerry's area.

South Bend: Barnes & Noble, Town & Country Shopping Center.

Kansas

Kansas City: Oak Park Mall food court (Overland Park).

Kentucky

Louisville: Barnes & Noble on Hurstbourne Pkwy.

Louisiana

Baton Rouge: In the LSU Union Building, between the Tiger Pause & McDonald's, next to the payphones. Payphone numbers: (225) 387-9520, 9538, 9618, 9722, 9733, 9735.

New Orleans: [illegible] Coffee House, 5335 Canal Blvd. 6 pm.

Maine

Portland: Maine Mall by the bench at the food court door.

Maryland

Baltimore: Barnes & Noble cafe at the Inner Harbor.

Massachusetts

Boston: Prudential Center Plaza, terrace food court. Payphones: (617) 236-6582, 6583, 6584, 6585, try to bypass the carrier.

Michigan

Ann Arbor: Michigan Union (University of Michigan), [illegible].

Minnesota

Bloomington: Mall of America, north side food court, across from Burger King & the bank of payphones that don't take incoming calls.

Duluth: Barnes & Noble by Cub [illegible]. 7 pm.

Missouri

St. Louis: Galleria, Highway 40 & Brentwood, elevated section, food court area, by the theaters.

Springfield: Barnes & Noble on Battlefield across from the mall.

Mississippi

Biloxi: Edgewater Mall food court, [illegible] at 2600 Beach Blvd. [illegible].

Nebraska

Omaha: Oak View Mall Barnes & Noble. 6:30 pm.

Nevada

Las Vegas: [illegible] Superstore Cafe, Sahara & Decatur. 8 pm.

Reno: Meadowood Mall, Palms food court by Sbarro. 3-5 pm.

New Hampshire

Nashua: Pheasant Lane Mall, near the big clock in the food court.

New Jersey

Wayne: Wayne Town Center Mall, by [illegible] and the [illegible] phone.

New Mexico

Albuquerque: Winrock Mall food court, near payphones on the lower level between the fountain & arcade. Payphones: (505) 883-9985, 9976, 9841.

New York

Buffalo: Galleria Mall food court.

New York: Citicorp Center, in the lobby, near the payphones, 153 E 53rd St., between Lexington & 3rd.

Rochester: Marketplace Mall food court. 6 pm.

North Carolina

Charlotte: South Park Mall, raised area in the food court.

Raleigh: Crabtree Valley Mall, food court.

Ohio

Akron: Arabica on W. Market Street, intersection of Hawkins, W. Market, and Exchange.

Cleveland: Coventry Arabica, Cleveland Heights, back room smoking section.

Columbus: [illegible] (downtown), basement, far end of building in carpeted payphone area.

Dayton: At the [illegible] behind the [illegible].

Oklahoma

Oklahoma City: Shepard Mall, at the entrance next to [illegible] Cafe (by payphones). Payphone numbers: (405) 942-9027, 9226, 9351, 9458.

Tulsa: Woodland Hills Mall food court.

Oregon

Portland: Pioneer Place Mall (not Pioneer Square!), food court. 6 pm.

Pennsylvania

Philadelphia: 30th Street Amtrak Station at 30th & Market, under the "Stairwell 7" sign. Payphones: (215) 222-9880, 9881, 9779, 9799, 9632; 387-9751.

South Dakota

Sioux Falls: Empire Mall, by Burger King.

Tennessee

Knoxville: Borders Books Cafe across from Westown Mall.

Memphis: Cafe Apocalypse.

Nashville: Bean Central Cafe, intersection of West End Ave. & 29th Ave. S. three blocks west of Vanderbilt campus.

Texas

Austin: Dobie Mall food court.

Dallas: Mama's Pizza, Campbell & Preston.

Ft. Worth: North East Mall food court near the payphones, Loop 820 @ Bedford Euless Rd. 6 pm.

Houston: Galleria 2 food court, under the stairs.

San Antonio: North Star Mall food court.

Utah

Salt Lake City: ZCMI Mall in the food court.

Vermont

Burlington: Borders Books at Church St. and Cherry St. on the second floor of the cafe.

Washington

Seattle: Washington State Convention Center. First floor.

Spokane: Spokane Valley Mall food court.

Wisconsin

Eau Claire: [illegible] Mall food court.

Madison: Union South (227 N. Randall Ave.) on the lower level in the Martin Luther King Jr. Lounge by the payphones. Payphone: (608) 251-9909.

Milwaukee: Mayfair Mall on Highway 100 (Mayfair Rd.) & North Ave. in the food court. Payphone: (414) 302-9549.

All meetings take place on the first Friday of the month from approximately 5 pm to 8 pm local time unless otherwise noted. To start a meeting in your city, leave a message & phone number at (631) 751-2600 or send email to meetings@2600.com.

IT'S NOT OVER!

MPAA
2600
R.PASTE

The MPAA may have won their lawsuit against 2600 but the bigger battle is only just beginning. We're taking this fight to the Appellate Court and, if necessary, all the way to the Supreme Court! We need your support now more than ever.

You can help spread the word by sporting our stylish anti-MPAA t-shirt. The front looks a lot like the cover to our Spring 2000 issue while the back has the above scary caricature of MPAA chief Jack Valenti.

The shirts are $25 each, the proceeds of which go to the defense fund. In addition, we have "Stop the MPAA" bumper stickers (10 for $10) and "Stop the MPAA" buttons (3 for $10). Please show your support and help send a message that this affront to all of our rights won't be tolerated.

You can order all of these items plus our regular stuff through our online store at www.2600.com or by writing to us at:

2600
PO Box 752
Middle Island, NY 11953
U.S.A.